

10/531/12

Rec'd PCT/PTO 18 APR 2005

PCT/JPO3/13218

日本国特許庁
JAPAN PATENT OFFICE

15.10.03
RECEIVED
04 DEC 2003
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 Date of Application: 2002年11月25日

出願番号 Application Number: 特願2002-340582

[ST. 10/C]: [JP2002-340582]

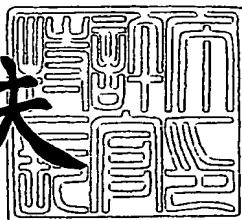
出願人 Applicant(s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年11月21日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

出証番号 出証特2003-3096364

【書類名】 特許願
【整理番号】 2054041316
【提出日】 平成14年11月25日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 29/10
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 森岡 芳宏
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 綾木 靖
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 三谷 浩
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 白木 直司
【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社
【代理人】
【識別番号】 100097445
【弁理士】
【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 パケット送受信装置

【特許請求の範囲】

【請求項 1】 送信装置と受信装置の間でデータのパケット通信を行なうパケット送受信装置であって、

認証と鍵交換の設定に関する情報を入力し、前記送信装置と受信装置の間での認証と鍵交換を行ない送信データの暗号化鍵または受信データの復号鍵の少なくとも一つを出力するAKE手段と、

送信データを入力し、前記AKE手段より与えられる暗号化鍵を用いて前記送信データを暗号化して出力する暗号化手段と、

送信データの送信条件に関する情報、送受信管理情報、および受信条件に関する情報の少なくとも一つの情報を入力し、パケットの送信条件を設定管理する送信条件の設定管理手段と、

前記送信条件の設定管理手段より入力される設定情報および前記AKE手段より入力されるAKEに関する情報の少なくとも一つを用いて、前記暗号化手段の出力をパケット化して出力するパケット化手段と、

受信パケットの受信条件に関する情報およびパケット受信状況に関する情報の少なくとも1つを入力し、受信条件の設定管理を行なう受信条件の設定管理手段と、

前記送信条件の設定管理手段より入力される設定情報を用いて、入力される受信パケットを受信データに変換し出力するとともに、前記受信パケットより生成する情報を前記AKE手段または前記受信条件の設定管理手段の少なくとも一つに出力するパケット受信手段と、

前記パケット受信手段より出力される受信データを入力し、前記AKE手段より与えられる暗号の複合鍵を用いて前記受信データを復号して受信データを出力する復号手段とを具備することを特徴とするパケット送受信システム。

【請求項 2】 前記パケット化手段の出力を入力し、フレームに変換して出力するフレーム化手段と、受信フレームを入力し、パケットに変換して出力するフレーム受信手段とを具備することを特徴とする請求項1記載のパケット送受信装置

【請求項3】前記送信条件の設定管理手段より送信キューの送信制御情報を入力し、送信キューに蓄積されたデータ状況をモニタしながら送信制御を行なう送信キュー制御手段と、

前記パケット化手段の第1のパケット出力を入力し一時的に蓄積し、前記送信キュー制御手段の制御により蓄積したパケットを出力する第1キュー手段と、

前記パケット化手段の第2のパケット出力を入力し一時的に蓄積し、前記送信キュー制御手段の制御により蓄積したパケットを出力する第2キュー手段と、

前記第1キュー手段と第2キュー手段の出力パケットを入力し、フレームに変換して出力するフレーム化手段と、受信フレームを入力し、パケットに変換して出力するフレーム受信手段とを具備することを特徴とする請求項1記載のパケット送受信装置。

【請求項4】前記送信キューの送信制御情報は、入力されるパケットの送信経路に関する情報、パケット送信に必要な帯域幅に関する情報、前記パケット送信手段から前記パケット受信手段までの遅延に関する情報、パケット送信の優先度に関する情報のうち少なくとも1つの情報を用いて、

前記第1キュー手段と前記第2キュー手段に蓄積されたデータの送信制御を行なうことを特徴とする請求項3記載のパケット送受信装置。

【請求項5】前記データの送信制御は、IETF rfc2205、rfc2208、rfc2209で記載されているRSVP方式、IETF rfc2210、rfc2211、2212、rfc2215で記載されているIntserv方式、IETF rfc2474、rfc2475、rfc2597、rfc2598で記載されているDiffServ方式のいずれか1つの制御方式を使用することを特徴とする請求項4記載のパケット送受信装置。

【請求項6】前記送信キュー制御手段は、前記第1キュー手段と前記第2キュー手段に蓄積されたデータのうち、前記第1キュー手段または前記第2キュー手段に蓄積されたデータのいずれかを選択して、優先出力するように制御することを特徴とする請求項3記載のパケット送受信装置。

【請求項7】前記送信キュー制御手段は、

前記第2キュー手段に蓄積されるデータ量が特定の範囲を超えない場合には、前記第1キュー手段に蓄積されたデータを優先して出力し、

前記第2キュー手段に蓄積されるデータ量が特定の範囲を超えた場合には、前記第2キュー手段に蓄積されたデータを優先して出力するように制御することを特徴とする請求項3記載のパケット送受信装置。

【請求項8】前記送信キュー制御手段は、前記第1キュー手段と前記第2キュー手段から出力されるデータの出力間隔を平均化するように制御することを特徴とする請求項3、4、5、6、7記載のパケット送受信装置。

【請求項9】前記送信データの設定管理手段と前記受信条件の設定管理手段は、送信手段と受信手段間で送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、前記最大伝送パケットサイズ情報を用いて、前記パケット化情報を生成することを特徴とする請求項1に記載の送信装置。

【請求項10】前記フレーム化手段は、前記パケット化手段より入力されるパケットに、IEEE 802.3規格のフレームヘッダーを付加することを特徴とする請求項1記載の送信装置。

【請求項11】前記フレーム化手段は、前記パケット化手段より出力されるパケットに、IEEE 802.1Q規格のフレームヘッダーを付加することを特徴とする請求項1記載の送信装置。

【請求項12】前記パケット化手段は、入力されるデータを特定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIP (Internet Protocol) ヘッダーを付加することを特徴とする請求項1記載の送信装置。

【請求項13】前記パケット化手段は、IPv4ヘッダーのサービスタイプフィールド、または、サービスタイプフィールド内のTOS (Type of Service) フィールドに優先パケットであることを示す情報を付加することを特徴とする請求項1記載の送信装置。

【請求項14】前記パケット化手段は、IPv6ヘッダーのプライオリティフィールドに優先パケットであることを示す情報を付加することを特徴とする請求

項1記載の送信装置。

【請求項15】前記パケット化手段は、第一のパケット化手段、および、第二のパケット化手段により構成され、

第一のパケット化手段は、前期送信条件の設定管理手段より入力される設定情報を用いて、前期送信条件の設定管理手段より入力される設定情報と前記A K E手段より入力されるA K Eに関する情報の少なくとも一つの情報を用いてパケット化して出力し、

第二のパケット化手段は、前期送信条件の設定管理手段より入力される設定情報を用いて、前記A K E手段より入力されるA K Eに関する情報と前記暗号化手段の出力の少なくとも一つの情報を用いてパケット化して出力することを特徴とする請求項3記載のパケット送受信装置。

【請求項16】前記第一のパケット化手段はソフトウェアにより処理され、前記第二のパケット化手段はハードウェアにより処理されることを特徴とする請求項12のパケット化手段に入力することを特徴とする請求項15記載のパケット送信装置。

【請求項17】入力データを優先データと一般データに分離するデータ分離手段を具備し、前記優先データを前記暗号化手段に入力し、また、前記一般データを前記第1のパケット化手段に入力することを特徴とする請求項15記載のパケット送信装置。

【請求項18】前記第一のパケット化手段はI E T F文書で規定されているデータ処理プロトコルであるR T C P, R T S P, T C P、U D P、I Pのうちの少なくとも1つのヘッダーを附加することを特徴とする請求項17記載のパケット送受信装置。

【請求項19】前記第二のパケット化手段は、入力データにシーケンス番号の附加、または、I E T F文書で規定されているデータ処理プロトコルであるR T P, U D P、I Pのうちの少なくとも1つのヘッダーの附加を行なうことを特徴とする請求項17記載のパケット送受信装置。

【請求項20】前記優先データは、S M P T E 2 5 9 M規格で規定された非圧縮S D方式信号、または、S M P T E 2 9 2 M規格で規定された非圧縮H D

形式、または、IEC 61883規格で規定されたIEEE1394によるDVまたはMPEG-TSの伝送ストリーム形式、または、DVB規格A010で規定されたDVB-ASIによるMPEG-TS形式の内の少なくとも一つのデータストリーム形式であることを特徴とする請求項17記載のパケット送信装置。

【請求項21】前記第二のパケット化手段はエラー訂正符号の付加手段を具備していることを特徴とする請求項15記載のパケット送受信装置。

【請求項22】前記エラー訂正符号の付加手段で用いるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式であることを特徴とする請求項21記載のパケット送受信装置。

【請求項23】前記暗号化鍵情報は、前記フレーム化手段より前記暗号化鍵で暗号化されたパケットを出力されるより以前のタイミングで、前記暗号化鍵の復号情報を前記フレーム化手段より出力し、前記受信手段に知らせることを特徴とする請求項15記載のパケット送信装置。

【請求項24】前記暗号化鍵情報を出力するタイミングは、前記暗号化鍵で暗号化されたパケットが前記送信手段からの出力されるタイミングよりも、前記送信手段と前記受信手段間のパケット往復伝播および処理時間よりも大きいことを特徴とする請求項23記載のパケット送信装置。

【請求項25】前記AKE処理手段は、DTLAで規定されているDTCP方式に準拠した手順で認証と鍵交換が行ない、特定の期間で更新される暗号化鍵または復号鍵を出力することを特徴とする請求項1から24記載のパケット送受信装置。

【請求項26】前記AKE処理手段におけるD TCP方式の復号鍵の更新タイミングの送信側から受信側への通知は、伝送されるパケット自身に更新タイミング情報を附加して送信することにより行なうことを特徴とする請求項25記載のパケット送受信装置。

【請求項27】前記AKE処理手段におけるD TCP方式の復号鍵の更新タイミングの送信側から受信側への通知は、暗号化されて伝送されるパケットのTCPポート番号、またはUDPポート番号を変化させることにより行なうことを特

徴とする請求項25記載のパケット送受信装置。

【請求項28】前記AKE処理手段におけるD TCP方式のコピー制御情報の伝送は、送信側から受信側へ伝送されるパケット自身にコピー制御情報を附加して送信することを特徴とする請求項25記載のパケット送受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、IEEE 802.3などのイーサネット(R)(有線LAN)やIEEE 802.11などの無線LANなどを用いて、暗号化されたAVストリームをIPパケット化して高品質に送受信するパケット送受信装置に関する。

【0002】

【従来の技術】

従来、一般家庭において、IEEE 1394を用いて、IEC 61883-4で規定された方式に基づきMPEG-TS信号の暗号化伝送が行なわれている。MPEG-TSなどAVデータを暗号化して伝送する方式の一例として、D TCP(Digital Transmission Content Protection)方式が規定されている。D TCPは、IEEE 1394やUSBなどの伝送メディア上のコンテンツ保護技術である。D TCP方式は、DTLA(Digital Transmission Licencing Administrator)で規格化された方式であり、<http://www.dtcp.com>、http://www.dtcp.com/data/dtcp_tut.pdf、http://www.dtcp.com/data/wp_spec.pdfや、書籍「IEEE 1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、kopープロテクション」、133~149ページで説明されている。

【0003】

図18は、D TCP方式を用いたMPEG-TSのIEEE 1394での伝送の一例である。D TCP方式では、送信側をソース(2001)、受信側をシンク(2002)と呼び、暗号化したMPEG-TSなどのコンテンツをソース(2001)からネットワーク(2003)を介して、シンク(2002)へ伝送している。図18に、補足情報として、ソース機器およびシンク機器の例を併記する。

【0004】

次に、図19を用いて、D TCP方式における従来のパケット通信手段の概略を説明する。図19は図18のソース（2001）、およびシンク（2002）の構成の概略図である。まず、D TCP方式に準拠した認証と鍵交換（Authentication and Key Exchange、AKEと略す）が行なわれる。AKE手段（認証と鍵交換手段）1901に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段1902により規定のヘッダーを付加されパケット化され、ネットワークに出力される。ここで、パケット化手段1902は送信条件設定手段1903により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワークより入力する信号がパケット受信手段1904でパケットヘッダーなどの識別によりフィルタリングされ、AKE手段1901に入力される。これにより送信側（ソース）のAKE手段と、受信側（シンク）のAKE手段がネットワークを介してお互いにメッセージの通信ができる。すなわち、D TCP方式の手順い従い、認証と鍵交換を実行する。なお、本明細書では、AKE手段を介してコンテンツ伝送を行なう送信側をソースと呼び、受信側をシンクと呼ぶ。

【0005】

送信側（ソース）と、受信側（シンク）で認証と鍵交換が成立すれば、次に、AVデータの伝送を行なう。ソースでは、MPEG-TS信号を暗号化手段1905に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段1902に入力し、ネットワークに出力する。シンクでは、ネットワークより入力する信号がパケット受信手段1904でパケットヘッダーなどの識別によりフィルタリングされ、復号手段1906に入力され、復号されMPEG-TS信号が出力される。

【0006】

次に、図20を用い上記手順を補足説明する。図20において、ソースとシンク間はIEEE 1394で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護

情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはD TCP所定の処理により認証鍵の共有を図る。そして、ソースは認証鍵を用いて交換鍵を暗号化してシンクに送り、シンクで交換鍵が復号される。ソースでは暗号鍵を時間的に変化させるために、時間的に変化するシード情報を生成し、シンクに送信する。ソースでは、交換鍵とシード情報より暗号化鍵を生成して、MPEG-TSをこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたMPEG-TS信号を復号する。

【0007】

図21は、図18においてMPEG-TS信号を伝送する場合のIEEE 1394アイソクロナスパケットの一例である。このパケットは、4バイト(32ビット)のヘッダー、4バイト(32ビット)のヘッダーザーCRC、224バイトのデータフィールド、4バイト(32ビット)のトレイラによって構成されている。暗号化されて伝送されるのは224バイトのデータフィールドを構成するCIPヘッダーとTS信号のうち、TS信号のみで、他のデータは暗号化されない。ここで、D TCP方式固有の情報は、コピー保護情報である2ビットのEMI(Encryption Mode Indicator)、および1ビットのシード情報O/E(Odd/Even)であり、これらは上記32ビットのヘッダー内に存在するため暗号化されずに伝送される。

【0008】

【非特許文献1】

「IEEE1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピー・プロテクション」、133～149ページ

【0009】

【発明が解決しようとする課題】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来のD TCP方式はIEEE 1394において、アイソクロナスパケットを用いて伝送するためMPEG-TS信号のリアルタイム伝送ができるが、インターネット

トの標準プロトコルであるIPプロトコルを用いて、イーサネット（R）（IEEE 802.3）、無線LAN（IEEE 802.11）や、その他のIPパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。すなわち、IPプロトコルを介して論理的に接続された送信機器と受信機器の間を、暗号化によりコンテンツの機密性や著作権の保護を行なった状態でMPEG-TS信号などAVストリームを伝送できないという大きな問題点がある。

【0010】

【課題を解決するための手段】

上記課題を解決するために、本願第1の発明は、ネットワークを介して論理的に接続されたパケット送信手段とパケット受信手段は、MPEG-TS信号などの送信コンテンツの機密性や著作権を保護を実現するための機器認証と暗号化鍵の交換手段（AKE手段）と、コンテンツの暗号化手段、および、暗号化されたコンテンツの復号手段と、受信側からフィードバックされるパケット受信状況を入力して適切なパケット送信条件を設定するパケット送信条件設定管理手段と、パケット化手段と、パケット受信手段と、パケット受信条件の設定管理手段とを具備する。これにより、MPEG-TS信号などのAVストリームを送信機器で暗号化してデータの機密性や著作権の保護などを図り、IPパケットを伝送できるネットワークを介して伝送し、受信機器で元の信号を復号することが可能である。

【0011】

本願第2の発明は、第1の発明におけるパケット化手段において、送信パケットを一般パケットとリアルタイム性が高く優先送信されるパケットにクラス分けし、一般パケットを第1のデータキューに、また、優先送信されるパケットを第2のデータキューに入力する。そして、送信キュー制御手段により第1のデータキューおよび第2のデータキューに一時蓄積されているパケットの送信順序を制御する。これにより、データの機密性や著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。

【0012】

また、入力ストリームが2チャネル以上の複数ストリームの場合にも、各々の

ストリームに関する信号を優先データと一般データにクラス分けすることにより対応が可能である。

【0013】

本願第3の発明は、第2の発明におけるパケット化手段の内部構成として、第1のパケット化手段と第2のパケット化手段とを持つ。ここで、AKE設定に関するデータや一般データは第1のパケット化手段に入力される。また、暗号化手段の出力データおよびAKE情報はハードウェアによるパケット化が実行される第2のパケット化手段に入力される。なお、AKE情報とは、コピー制御情報や暗号化鍵の更新情報のことである。第1のパケット化手段の出力は前記第1のデータキューに入力され、第2のパケット化手段の出力は前記第2のデータキューに入力される。送信条件の設定管理手段より送信キュー制御手段に対して、第2データキューに一時蓄積されている信号を優先出力するコマンドを出すと、暗号化されたコンテンツが優先して出力される。この制御において、第2データキューがオーバフローしない様に制御すれば、受信側で適切な大きさのバッファを持つことにより、送受信機器間でコンテンツのリアルタイム伝送が実現できる。

以上、送受信機器間でコンテンツを暗号化してリアルタイム伝送する際に、第2のパケット化手段がハードウェアで構成されているため、ソフトウェア処理が間に合わないために発生する送信パケットの送り残しや受信パケットの取りこぼしといった不具合が発生しない。また、データ量の小さい第1のパケット化手段は安価なマイコンなどでも構成できるため、低コスト化が図れる。

【0014】

本願第4の発明は、第3の発明において、機器認証と暗号化鍵の交換を行なうAKE手段は、DTCPIP方式に基づいた方式であり、暗号化鍵生成手段と、AKE情報生成手段と、AKEコマンド送信処理手段と、AKEコマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを具備する。暗号化鍵生成手段は、暗号化鍵を生成し暗号化に入力し暗号化動作を設定する。AKE情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報とを入力しAKE情報を生成する。AKEコマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部よりA

KEパラメータを、さらにAKEコマンド受信処理手段よりAKEコマンド情報を受け取り、AKE送信コマンドを生成し出力する。AKEコマンド受信処理手段は、第1のパケット受信手段よりAKE設定制御情報を受け取り、AKE送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、AKEコマンド受信処理手段と第1のパケット受信手段より情報を得て暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号鍵変更情報生成手段より情報を入力し復号鍵を生成し復号手段に出力する。

【0015】

本願第5の発明は、第2の発明において、暗号化手段の出力データ、および、コピー制御情報や暗号化鍵の更新情報などのAKE情報が入力される第2のパケット化手段が、内部にエラー訂正符号の付加手段を具備し、これらの情報にエラー訂正符号を付加し、UDP／IPプロトコルにより伝送される。これにより、IPパケットの伝送において、ネットワークでパケットロスやビットエラーなどが発生した場合にも、受信側でエラー訂正により送信データの復元が可能となる。

【0016】

【発明の実施の形態】

まず最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図1は本願発明を適用するシステムの一例である。

図1において、パケット送信機器101およびパケット受信機器103は、本願第1，2，3、4および5の発明実施部である（以下、本願発明部）。101は送信機器、102はルータ、103は受信機器である。送信機器101には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム（MPEG-TSなどコンテンツ）が入力され、以下の手順1から3に基づき、通信が実行される。

手順1) 送受信パラメータの設定を行なう。

(1-1) 送受信機器のMACアドレス、IPアドレス、TCP／UDPポート番号等を設定。

(1-2) 送信信号の種別、帯域を設定。QoSエージェントとして動作する送信機器101と受信機器103、QoSマネージャとして動作するルータ102との間でIEEE 802.1Q (VLAN) 規格を用いたネットワークの運用に関する設定を実施。

(1-3) 優先度の設定 (IEEE 802.1Q/pによる運用)

手順2) 認証と鍵交換：

(2-1) 認証と鍵交換を行なう。たとえば、TCP方式を用いることもできる。

手順3) ストリーム伝送：

(3-1) 送信機器と受信機器間での暗号化されたストリームコンテンツ (MPEG-TS) の伝送

なお、コンテンツの入力信号として、例ではMPEG-TSを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム (ISO/IEC 13818) 、DV (IEC 61834、IEC 61883) 、SMPTE 314M (DV-based) 、SMPTE 259M (SDI) 、SMPTE 305M (SDTI) 、SMPTE 292M (HD-SDI) 等で規格化されているストリームなお、一般的なAVコンテンツも適用可能である。さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

次に、上記手順2の認証と鍵交換に関して補足説明する。図2において、送信機器と受信機器間はIPネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式決定して認証要求を送信機器に送る。これらの処理を通して送信機器と受信機器は認証鍵を共有する。次に、送信機器は認証鍵を用いて交換鍵を暗号

化して受信機器に送り、受信機器で交換鍵が復号される。送信機器では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、受信機器に送信する。送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、MPEG-TSをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたMPEG-TS信号を復号する。

【0017】

図3は本方式をイーサネット（R）を用い2階建ての家庭に適用した場合の一例である。図3において、301は1階のネットワーク構成、302は2階のネットワーク構成である。303は1階に設置されインターネットと接続されるルータ、304は2階に設置されているスイッチングハブである。304はルータ303とスイッチングハブ304を接続するイーサネット（R）ネットワークである。家庭なの全てのイーサネット（R）ネットワークの帯域は100Mbpsである。1階のネットワーク構成の詳細としては、ルータ303にはテレビ（TV）、パソコン（PC）、DVDレコーダが100Mbpsのイーサネット（R）で接続され、また、エアコン、冷蔵庫がECHONETで接続されている。また、2階では、スイッチングハブ304にテレビ（TV）、パソコン（PC）、DVDレコーダが100Mbpsのイーサネット（R）で接続され、また、エアコンがECHONETで接続されている。なお、ECHONETは「エコーネットコンソーシアム」(<http://www.echonet.gr.jp/>)で開発されている伝送方式である。

【0018】

図3において、パソコン（PC）、DVDレコーダ、ルータ301およびスイッチングハブ304は、IEEE 802.1Q（VLAN）に対応している。すなわち、ルータ301およびスイッチングハブ304において、各ポートのデータレートが全て同じ（例えば100Mbps）場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ（あるいは、スイッチングハブ）内部で失われず全て出力ポートに出力される。スイッチングハブでは、たとえば8

個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

【0019】

図3において、家庭内の全てのイーサネット（R）の帯域が100Mbpsであるため、1階と2階間のネットワーク305の帯域も100Mbpsである。1階と2階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク305上を流れるデータのデータレート合計が100Mbpsを超える可能性があり、MPEG-TSの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。たとえば、MPEG-TSストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することが可能となる。

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。すなわち、ルータ（あるいは、スイッチングハブ）の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジューリング方式WF-FQ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する情報は、戸田巖著、「ネットワークQoS技術」、平成13年5月25日（第1版）、オーム社刊の第12章などに記述されている。

(実施の形態1)

本願第1の発明について説明する。図4は本願第1の発明のパケット送受信手段に関するブロック図である。401はAKE手段を用いた暗号化によるパケット送受信手段である。AKE手段402に対してAKE設定情報を入力され、このAKE設定情報に関連した情報、たとえばコピー保護情報と暗号化鍵変更情報、がパケット化手段403に入力され、TCP/IPプロトコルのヘッダーを付加され、さらに、フレーム化手段409においてMACヘッダーが付加されイーサネット(R)フレームに変換し、送信フレームとしてネットワークに出力される。ここで、パケット化手段403は送信条件設定手段404により決定された送信パラメータにより、入力データのパケット化および送信を行なう。なお、送信条件設定手段404には、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段(ローカル)と受信手段(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段403およびフレーム化手段409で生成するヘッダーやペイロードデータなどを設定する。

受信側では、ネットワークより入力する信号がフレーム受信手段410でMACヘッダーを元にフィルタリングされ、IPパケットとしてパケット受信手段405に入力される。パケット受信手段405ではIPパケットヘッダーなどの識別によりフィルタリングを行い、AKE手段402に入力される。これにより送信側のAKE手段と、受信側のAKE手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、AKE手段の設定手順に従い、認証と鍵交換を実行することができる。

【0020】

送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。送信側では、MPEG-TS信号を暗号化手段406に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段403に入力し、TCP/IPプロトコルのヘッダーを付加する。さらに、フレーム化手段409において、802.1Q(VLAN)方式を用いて、M

ACヘッダーを付加しイーサネット（R）フレームに変換して、送信フレームとしてネットワークに出力する。ここで、MACヘッダー内のTCI（Tag Control Information）内のPriority（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。受信側では、ネットワークより入力する信号がフレーム受信手段410でMACヘッダーを元にフィルタリングされ、IPパケットとしてパケット受信手段405に入力される。パケット受信手段405でパケットヘッダーなどの識別によりフィルタリングされ、復号手段407に入力され、復号されたMPEG-TS信号が出力される。

【0021】

なお、送信条件設定手段404には、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段403およびフレーム化手段409で生成するヘッダーおよびペイロードデータを設定する。

【0022】

次に、図5のプロトコルスタックを用い上記手順を補足説明する。図5の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ID、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるMPEG-TSは暗号化鍵により暗号化される。そして暗号化されたMPEG-

T Sは、前述したEMI、O/EとともにAVデータとしてTCP（またはUDP）パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット（R）MACフレームが生成される。なお、MACとしてはイーサネット（R）であるIEEE 802.3だけでなく、無線LAN規格のIEEE 802.11のMACにも適用できる。

【0023】

さて、イーサネット（R）MACフレームは、イーサネット（R）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（R）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP（またはUDP）パケットが抜き出される。そして、TCP（またはUDP）パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG-TS（コンテンツ）が復号され出力される。

【0024】

以上、MPEG-TS信号などのAVストリームを送信機器で暗号化して、IPパケットをネットワークにより伝送し、受信機器で元の信号に復号することが可能である。

なお、図3において、スイッチングハブを用いたネットワークトポロジーを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。たとえば、1階と2階の間のネットワーク305の帯域を、従来の実施例で説明した100Mbpsから1Gbpsに拡張することによって、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することができる。たとえば、市販されている100Mbpsのポートを8つ、1Gbpsのポートを1つ持ったスイッチングハブを用い、1階と2階を結ぶネットワーク305に1Gbpsのポートを接続し、残りの8chの100MbpsのポートにTVなどのAV機器を接続する。100Mbpsのポートは8

つなので、8つのポートのデータがそれぞれ最大100Mbpsで入力されて1Gbpsのポートに出力されたとしても、 $100\text{Mbps} \times 8\text{ch} = 800\text{Mbps}$ と1Gbpsより小さいため、8つのポートから入力されたデータはスイッチングハブ内部で失われず全て1Gbpsのポートに出力される。よって、1階で発生したデータは全て2階に伝送することが可能である。また、逆に2階で発生したデータも全て1階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークトポロジーを工夫することによりストリーム伝送とファイル転送を共存させることができる。

(実施の形態2)

本願第2の発明について説明する。図6は本願第2の発明のブロック図である。図6においては、送信キュー制御手段601、第1キュー手段602、および第2キュー手段603以外は、図4と同様の構成である。よって以下では新規な部分について説明する。

図4において、AKE手段402に対してAKE設定情報を入力され、このAKE設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段403に入力され、TCP/IPプロトコル処理をして、第1キュー手段603に入力される。また、送信側ではMPEG-TS信号を暗号化手段406に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段403に入力し、TCP/IPプロトコル処理をして、第2キュー手段604に入力される。

送信キュー制御手段602は、第1キューと第2キューにデータが存在する場合、どちらのデータを優先して出力するかの制御を行なう。通常状態では、一般データよりもMPEG-TSなどのコンテンツデータを優先制御して出力する。たとえば、送受信機器間でMPEG-TSを低レイテンシ（低遅延）で伝送する場合には、MPEG-TS用バッファも小さくなるため、オーバーフローが発生し

やすい。送信側でMPEG-TSバッファがオーバーフローしそうになった場合、あるいは、受信側からフィードバックされた情報を参照して受信側のMPEG-TSのバッファがアンダーフローしそうになったことが判明した場合には、MPEG-TSデータを優先出力する様に第2キュー手段の優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。

ただし、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くするには、第1キューの優先度を適応的に上げればよいが、これでは前述したMPEG-TSバッファのオーバーフロまたはアンダーフローが発生する可能性がある。

バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くする別手段として、機器制御用パケットだけはキューを経由せずに直接フレーム化手段に出力する方法により、迅速な制御応答が実現できる。あるいは、機器制御用パケットに対して第3キューを新たに用意する方法により、迅速な制御応答が実現できる。

【0025】

受信側の動作は第1の実施例と同様である。

（実施の形態3）

本願第3の発明について説明する。図7は本願第3の発明のブロック図である。図7においては、パケット化手段403内の第1のパケット化手段701および第2のパケット化手段702、パケット受信手段405内の第1のパケット受信手段703および第2のパケット受信手段704以外は図6と同様の構成である、よって以下では新規な部分について説明する。

図7において、AKE手段402に対してAKE設定情報を入力し、このAKE設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが第1のパケット化手段701に入力されプロセッサーを用いたソフトウェア

処理でTCP/IPプロトコル処理をされ、第1キュー手段603に入力される。

送信側ではMPEG-TS信号を暗号化手段406に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段403に入力し、ハードウェア処理によりUDP/IPプロトコルの処理をされ、第2キュー手段604に入力される。

送信キュー制御手段602は、第1キューと第2キューの双方にデータが存在する場合、前述の実施の形態2と同様に、2つのキューからのデータ出力に関して優先制御を行なう。

さて、受信側では、ネットワークより入力する信号がフレーム受信手段410でMACヘッダーを元にIPパケットがフィルタリングされる。ここでは、上記第1のパケット化手段701から出力されたIPパケットが第1のパケット受信手段703に入力され、上記第2のパケット化手段702から出力されたIPパケットがおよび第2のパケット受信手段704に入力される。第1のパケット受信手段703ではプロセッサーを用いたソフトウェア処理でTCP/IPプロトコルの受信処理を行い、AKE手段402または受信条件の設定管理手段408に出力する。また、第2のパケット受信手段704ではハードウェア処理によりUDP/IPプロトコルの受信処理を行い、復号手段407に入力され、暗号が復号されたMPEG-TSが出力される。

次に、図8のプロトコルスタックを用い、上記手順を補足説明する。図8においては、MPEG-TSなどAVデータのトランスマッショング層がUDPである以外は、図5と同様の構成である、よって以下では新規な部分について説明する。図8の送信側において、コンテンツであるMPEG-TSは暗号化鍵Kcにより暗号化される。そして暗号化されたMPEG-TSは、前述したEMI、O/EとともにAVデータとして、ハードウェアによりUDPパケットのペイロードとしてUDPパケットが生成される。さらにこのUDPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。

なお、送信側から受信側への、EMI、O/E情報の伝送方法としては、たとえば、専用の別パケットを生成して伝送することも可能であり、暗号鍵復元がさら

に困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなど公衆網において、リアルタイムに伝送されるAVデータの暗号化パラメータが変化させたり、別パケットで送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては図5の例と同様に、ソフトウェア処理によりTCPパケットが生成され、IPパケット化される。

【0026】

さて、イーサネット（R）MACフレームは、イーサネット（R）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（R）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからUDPパケットが抜き出され、UDPパケットからAVデータが抜き出され、交換鍵とシード情報より復元された復号鍵Kcにより、MPEG-TS（コンテンツ）が復号され出力される。

【0027】

図9は、MPEG-TSをIPパケット化、さらにイーサネット（R）フレーム化して伝送する場合のパケット形式の一例である。188バイトのMPEG-TSに6バイトのタイムコード（TC）を付加して194バイトの単位を作る。TCは42ビットのタイムスタンプと6ビットのベースクロックID（BCID）により構成される。BCIDによりタイムスタンプの周波数情報を表すことができる。たとえば、（ケース1）BCIDが0x00の場合は、タイムスタンプの周波数情報はない、（ケース2）BCIDが0z01の場合は、タイムスタンプの周波数情報としては27MHz（MPEG2のシステムクロック周波数）である、（ケース3）また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz（MPEG1で使用されるクロック周波数）である、（ケース4）BCIDが0x03の場合は、タイムスタンプの周波数情報としては24.576MHz（IEEE 1394で使用されるクロック周波数）である。（ケース5）BCIDが0x04の場合は、タイムスタンプの周波数情報としては100MHz（イーサネット（R）で使用される周波数）である、という様にBCIDでタイムスタンプの周波数情報を表すことができる。194バイト単位のデータを2つあわせて暗号化して、更に2バイトのDSCP情報と合わせ

てRTPプロトコルのペイロードとする。ここで、D TCP情報は、2ビットのEMIと、1ビットのO/Eと13ビットのReserved Dataにより構成される。 RTPパケットはUDPおよびIPプロトコルによりパケット化された後、イーサネット(R)フレーム化される。イーサネット(R)ヘッダとしては、図9に示す様に、標準的なイーサネット(R)ヘッダーとIEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーの両方をサポートする。なお、IEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーにおけるTCIフィールドの中の3ビットのPriorityフラグにより、イーサネット(R)フレームの優先度を設定することができる。

【0028】

以上により、送受信機器間でMPEG-TS信号を暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。

さらに、ハードウェア処理により、受信処理においても、イーサネット(R)フレームを受信して、3層のIPヘッダー、4層のUDPヘッダを同時に検査することもできる。MPEG-TSパケットと一般データパケットを分離し、MPEG-TSパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

【0029】

パケットの送信タイミング、あるいは2つの送信データキューからのデータ送信割合をソフトウェアではなくハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチ

ングハプでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

(実施の形態4)

本願第4の発明について説明する。図10は本願第4の発明のブロック図であり、AKE手段にTCP方式を用いる場合の一例である。図10において、AKE手段402内のTCP情報生成手段1001、AKEコマンド受信処理手段1002、AKEコマンド送信処理手段1003、交換鍵生成手段1004、暗号鍵生成手段1005、暗号鍵変更情報生成手段1006、復号鍵生成手段1007以外は図8と同様の構成である、よって以下では新規な部分について説明する。図10においては、以下のステップでTCP方式により暗号化コンテンツの伝送が行なわれる。

(ステップ1) コピー制御情報がTCP情報生成手段1001に入力される。

(ステップ2) まず、ソース側でコンテンツの送信要求を発生させ、TCP情報生成手段1001よりコンテンツの保護モード情報(EMI情報)が第1のパケット化手段701に出力され、パケット化された後、ソースに送信される。

(ステップ3) そして、受信側(シンク)は、第1のパケット化手段703よりAKEコマンド受信処理手段1002に入力されたコンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、AKE送信処理手段1003を通じて認証要求をソースに送る。

(ステップ4) ソースとシンク間でTCP所定の処理が行なわれ、認証鍵が共有される。

(ステップ5) 次に、ソースはAKE送信処理手段において、認証鍵を用いて交換鍵を暗号化して第1のパケット化手段を経由してシンクに送り、シンクにおいてAKEコマンド受信処理手段から与えられる情報により、交換鍵生成手段1004において交換鍵が復号される。

(ステップ6) ソースでは暗号鍵を時間的に変化させるために、暗号化鍵生成手段において、時間的に変化するシード情報(O/E)を生成し、TCP情報生成手段1001、および第1のパケット化手段701を経由してシンクに送信する。

(ステップ7) ソースでは、暗号化鍵生成手段1005において交換鍵とシード情報より暗号化鍵を生成して、暗号化手段でMPEG-TSを案の具かして第2のパケット化手段702に出力する。

(ステップ8) シンク内部の、暗号鍵変更情報生成手段1006は第1のパケット受信手段703よりシード情報を受信し、復号鍵生成手段1007はこのシード情報と交換鍵生成手段1004の情報より復号鍵を復元する。

(ステップ9) シンクでは、この復号鍵を用いて復号手段407において、暗号化されたMPEG-TS信号を復号する。

【0030】

図11は、パケット化手段403内の第1のパケット化手段701および第2のパケット化手段702、パケット受信手段405内の第1のパケット受信手段703および第2のパケット受信手段704におけるパケット処理について説明する図である。

第1のパケット化手段701、入力データを内部でRTCPまたはRTSPプロトコル、TCPまたはUDPプロトコル、さらにIPプロトコルによる処理がなされ出力される。なお、RTCPプロトコル(rfc1889)は、ネットワークの実効帯域幅や遅延時間などを受信装置より送信装置に送り、送信装置は報告された通信状態に合わせて RTPで送信するデータの品質を調整して送信することもできる。また、RTSPプロトコル(rfc2326)は、再生、停止、早送り、などの制御コマンドを送ることもでき、AVファイルよりデータをダウンロードしながらコンテンツを再生することが可能である。

【0031】

第2のパケット化手段702は、内部で入力データをRTPプロトコル、UDPプロトコル、そしてIPプロトコルでそれぞれ処理してIPパケットを出力する。

【0032】

また、第1のパケット受信手段703は、内部でフィルタリングなどIP受信処理、TCPまたはUDPプロトコルの受信処理、さらに、RTCPまたはRTSPプロトコルによる受信処理がなされたデータが出力される。

【0033】

また、第2のパケット受信手段704は、内部でフィルタリングなどIP受信処理、UDPプロトコルの受信処理、さらに、RTPプロトコルの受信処理がなされたデータが出力される。

【0034】

以上により、送受信機器間でMPEG-TS信号をTCP方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。

(実施の形態5)

本願第5の発明について説明する。図10は本願第5の発明のブロック図であり、さらに図12は、パケット化手段403内の第1のパケット化手段701および第2のパケット化手段702、パケット受信手段405内の第1のパケット受信手段703および第2のパケット受信手段704におけるパケット処理について説明する図である。本願第5の発明においては、図12の第2のパケット化手段1201、および第2のパケット受信手段1202以外は図11と同様の構成である、よって以下では新規な部分について説明する。

【0035】

第2のパケット化手段1201は、内部で入力データにエラー訂正処理を行ない、RTPプロトコル、UDPプロトコル、そしてIPプロトコルでそれぞれ処理してIPパケットを出力する。

【0036】

また、第2のパケット受信手段1202は、内部でフィルタリングなどIP受信処理、UDPプロトコルの受信処理、RTPプロトコルの受信処理、さらにエラー訂正復号処理を行いエラー訂正されたデータが出力される。

【0037】

図13は本願第5の発明のプロトコルスタックの説明図であり、送信処理では、AVデータにエラー訂正符号が付加され(ECCエンコード)、UDPプロト

コルに渡される。また、受信処理では、UDPプロトコル処理よりデータを受け取りエラー訂正をして上位層のAVデータとなる。

【0038】

エラー訂正方式の例を、図14および図15を使用して説明する。図14はエラー訂正方式がリードソロモン方式の場合である。MPEG-TSを2つ単位でエラー訂正インターリーブマトリックスに入力する。なお、各行にはシーケンス番号を2バイト使用する。そして、図14に示す様に、たとえば前述した2バイトのDTCP情報を用い、さらに、RTPヘッダ、UDPヘッダ、IPヘッダ、イーサネット(R)ヘダを附加してイーサネット(R)フレームを構成する。

【0039】

以上により、送受信機器間でMPEG-TS信号をTCP方式により暗号化し、さらにエラー訂正符号を附加しリアルタイム伝送が可能となる。さらに、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。

【0040】

ところで、図16にパケット送信手段、また、図17にパケット送信手段のブロック図を示す。これらは、それぞれ、MPEG-TSなどAVコンテンツの受信機能、または送信機能を省いた構成であり、その他は前述の送受信手段と同じ構成であり、実施の形態1から5に適用できる。送信または受信のみの機器に対して適用可能であり、低コスト化が図れる。

【0041】

なお、上述した実施の形態1から5においては、一般のIPネットワークなどパケットの順序性が保証されていない通信網で伝送する場合には、パケットにシーケンス番号を附加して送信し、受信側でシーケンス番号を用いて順序性の保証を行ってもよい。この順序性の保証は、OSIモデルの第4層以上、すなわち、RTPプロトコルやビデオ信号処理などで行なうことができる。

【0042】

なお、送信側側でハードウェア処理され伝送されたAV信号のパケットが、ネットワークでフラグメントされないため対策ができる。すなわち、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ（MTU）を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、RFCの規格では全ての端末は576バイトのサイズのIPパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のIPパケットではフラグメントが起こらない。したがってIPパケットのサイズが576バイト以下となるように、送信側側でハードウェア処理されるAV信号のパケットサイズを調整すればよい。なお、送信側側でハードウェア処理されるAV信号のパケットにフラグメントが起こらない場合は、受信したパケットがフラグメントされていれば全て一般パケットとして処理すればよい。なお、イーサネット（R）のIPパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはIPパケットの最大値以下でなければならることは言うまでもない。

【0043】

また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側側でハードウェア処理され伝送されたAV信号のパケットのIPヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではIPパケットを廃棄されることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信側で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態1から実施の形態6までは、通信網プロトコルとしてイーサネット（R）を例としたがこの限りではない。

【0044】

また、ビデオ信号処理の例として、実施の形態1から5ではMPEG-TSを用いたが、これに限らず本発明で用いる入力データの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム（ISO/IEC 13818）、

DV (IEC 61834、IEC 61883)、SMPTE 314M (DV-based)、SMPTE 259M (SDI)、SMPTE 305M (SDTI)、SMPTE 292M (HD-SDI) 等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。映像や音声のデータレートは、CBR (constant bit rate) に限るものではない。さらに、映像や音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本願発明から排除するものではない。

また、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、一定の条件化でリアルタイムより高速の伝送も可能である。

よって、インターネットの分野で一般にストリーミングと呼ばれているコンテンツ伝送方式も実現可能である。ストリーミング方式のコンテンツ伝送の場合、送信側から受信側のバッファへネットワークを介してTCP/IPやUDP/IPによりコンテンツデータを伝送し、受信側のバッファからコンテンツデータを比較的一定レートでデータを読み出すことにより受信側で連続したコンテンツの再生が実現できる。

また、SMPTE (www.smpte.org)において規格化されたGXFファイルフォーマット (SMPTE 360M) や、規格化が推進されているMXFファイルフォーマットに準拠したファイルの暗号化伝送にも適用可能である。

【0045】

【発明の効果】

本願第1の発明によれば、以下のような効果を有する。すなわち、本願第1の発明によるパケット送受信手段は、送信データのセキュリティを確保するためのAKE手段と、コンテンツの暗号化手段、および、暗号化されたコンテンツの復号手段と、受信側からフィードバックされるパケット受信状況を入力して適切なパケット送信条件を設定するパケット送信条件設定管理手段と、パケット化手段と、パケット受信手段と、パケット受信条件の設定管理手段とを具備する。

これにより、MPEG-TS信号などのAVストリームを送信機器で暗号化してデータの機密性や著作権の保護などを図りながら、IPパケットをネットワークを介して伝送し、受信機器で元の信号を復号することが可能である。

【0046】

本願第2の発明によれば、以下のような効果を有する。すなわち、本願第2の発明によるパケット送受信手段は、送信パケットを一般パケットと優先送信されるパケットにクラス分けし、一般パケットを第1のデータキューに、また、優先送信されるパケットを第2のデータキューに入力する。そして、送信キュー制御手段により第1のデータキューおよび第2のデータキューに一時蓄積されているパケットの送信順序を制御する。

これにより、データの機密性や著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。また、入力ストリームが2チャネル以上の複数ストリームの場合にも、それぞれのストリームに関する信号を優先データと一般データにクラス分けすることにより対応が可能である。

【0047】

本願第3の発明によれば、以下のような効果を有する。本願第3の発明は、パケット化手段の内部に、第1のパケット化手段と第2のパケット化手段とを持つ。ここで、AKE設定に関するデータや一般データは第1のパケット化手段に入力される。また、暗号化手段の出力データおよびAKE情報はハードウェアによるパケット化が実行される第2のパケット化手段に入力される。なお、AKE情報とは、コピー制御情報や暗号化鍵の更新情報のことである。第1のパケット化手段の出力は前記第1のデータキューに入力され、第2のパケット化手段の出力は前記第2のデータキューに入力される。送信条件の設定管理手段より送信キュー制御手段に対して、第2データキューに一時蓄積されている信号を優先出力するコマンドを出すと、暗号化されたコンテンツが優先して出力される。

これにより、第2データキューがオーバフローしない様に制御すれば、受信側で適切な大きさのバッファを持つことにより、送受信機器間でコンテンツのリアルタイム伝送が実現できる。送受信機器間でコンテンツを暗号化してリアルタイム伝送する際に、第2のパケット化手段がハードウェアで構成されているため、ソ

フトウエア処理が間に合わないために発生する送信パケットの送り残しや受信パケットの取りこぼしといった不具合が発生しない。また、データ量の小さい第1のパケット化手段は安価なマイコンなどでも構成できるため、低コスト化が図れる。

【0048】

本願第4の発明によれば、以下のような効果を有する。すなわち、本願第4の発明によるパケット送受信手段は、第3の発明において、AKE手段はD TCP方式で規定されている処理手順に準拠し、暗号化鍵生成手段と、AKE情報生成手段と、AKEコマンド送信処理手段と、AKEコマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを具備する。暗号化鍵生成手段は、暗号化鍵を生成し暗号化に入力し暗号化動作を設定する。また、AKE情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報を入力しAKE情報を生成する。AKEコマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部よりAKEパラメータを、さらにAKEコマンド受信処理手段よりAKEコマンド情報を受け取り、AKE送信コマンドを生成し出力する。AKEコマンド受信処理手段は、第1のパケット受信手段よりAKE設定制御情報を受け取り、AKE送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、AKEコマンド受信処理手段と第1のパケット受信手段より情報を得て暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号化鍵変更情報生成手段より情報を入力し復号鍵を生成し復号手段に出力する。

【0049】

これにより、D TCP方式に準拠したAKE手段を用いて、M P E P - T SなどAVストリームを暗号化してリアルタイムに伝送することが可能となり、コンテンツの著作権保護が図られる。

【0050】

本願第5の発明によれば、以下のような効果を有する。すなわち、本願第5の発明によるパケット送受信手段は、第2の発明において、暗号化手段の出力データ

タおよびA KE情報（コピー制御情報や暗号化鍵の更新情報）が入力される第2のパケット化手段が、内部にエラー訂正符号の付加手段を具備し、エラー訂正符号を付加、さらにUDP／IPプロトコルにより伝送される。

これにより、IPネットワークでパケットロスやビットエラーなどが発生した場合にも受信側でエラー訂正により送信データの復元が可能となる。また、第2のパケット化手段、および第2のパケット受信手段をハードウェアで構成することが容易となる。

また、本願第1から第6までの発明によれば、ネットワークを用いたAVコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（AVデータコンテンツ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるAVデータの販売、課金が可能となり、安全性の高いB-B、B-Cのコンテンツ販売流通が可能となる。

また、本願第3から第6までの発明によれば、AVコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りCPUを用いてソフトウェア処理を行う。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データ量に比べて非常に少ないので、マイコンなど安価なマイクロプロセッサーで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なCPUや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

【図面の簡単な説明】

【図1】

本願第1の発明を適用するシステムの一例を示す図

【図2】

認証と鍵交換にD TCP方式を適用する場合のコンテンツ伝送手順の説明図

【図3】

イーサネット（R）を用いる一般家庭に適用した場合の一例の説明図

【図4】

本願第1の発明のパケット送受信手段のブロック図

【図5】

本願第1の発明のプロトコルスタックによる説明図

【図6】

本願第2の発明のパケット送受信手段のブロック図

【図7】

本願第3の発明のパケット送受信手段のブロック図

【図8】

本願第3の発明のプロトコルスタックによる説明図

【図9】

本願第3の発明におけるMPEG-TSのイーサネット(R)フレーム構成仕様の例を示す図

【図10】

本願第4の発明のパケット送受信手段のブロック図

【図11】

本願第4の発明におけるパケット化手段およびパケット受信手段の説明図

【図12】

本願第5の発明におけるパケット化手段およびパケット受信手段の説明図

【図13】

本願第5の発明のプロトコルスタックによる説明図

【図14】

エラー訂正方式がリードソロモン方式である場合の説明図

【図15】

エラー訂正方式がパリティ方式である場合の説明図

【図16】

パケット送信手段のブロック図

【図17】

パケット送信手段のブロック図

【図18】

DTCP方式を用いたMPEG-TSのIEEE 1394での伝送の一例を示す図

【図19】

DTCP方式における従来のパケット通信手段の概略を説明するための図

【図20】

DTCP方式に準拠した認証と鍵交換を説明するための図

【図21】

図18においてMPEG-TS信号を伝送する場合のIEEE 1394アイソクロナスパケットの一例を示す図

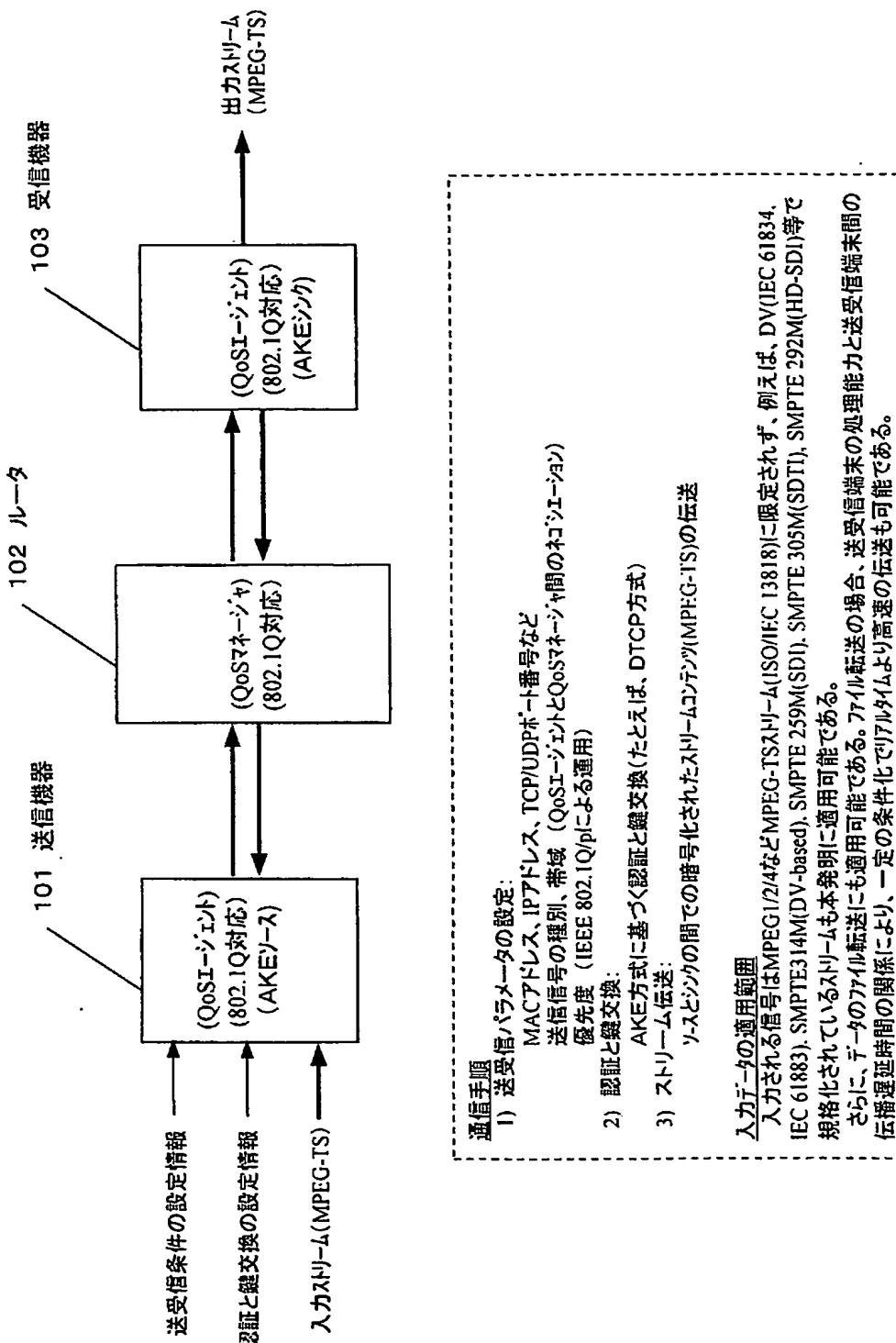
【符号の説明】

- 101 パケット送信機器
- 102 ルータ
- 103 パケット受信機器
- 401 パケット送受信手段
- 402 AKE手段
- 403 パケット化手段
- 404 送信条件の設定管理手段
- 405 パケット受信手段
- 406 暗号化手段
- 407 復号手段
- 408 受信条件の設定管理手段
- 409 フレーム化手段
- 410 フレーム受信手段

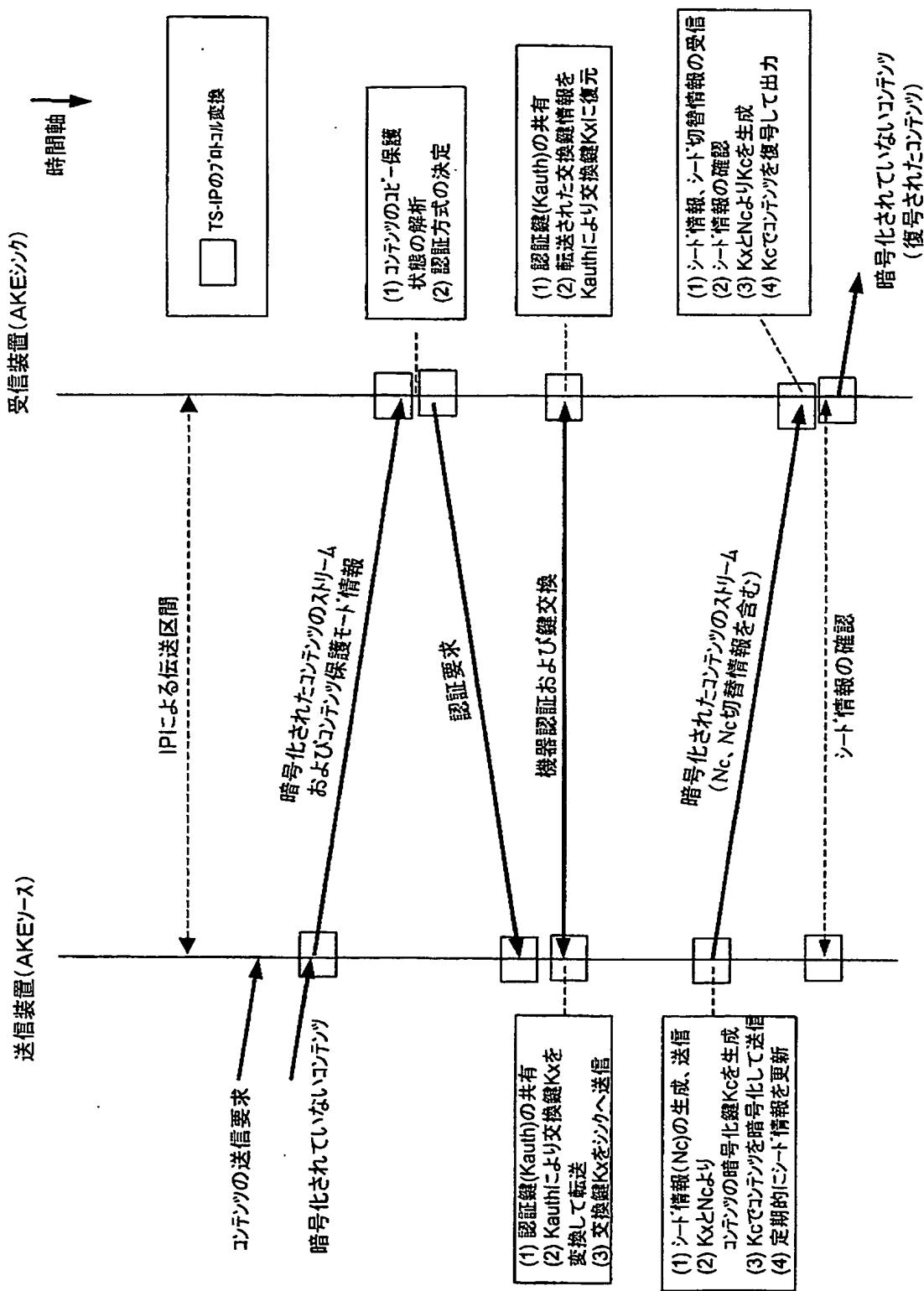
【書類名】

図面

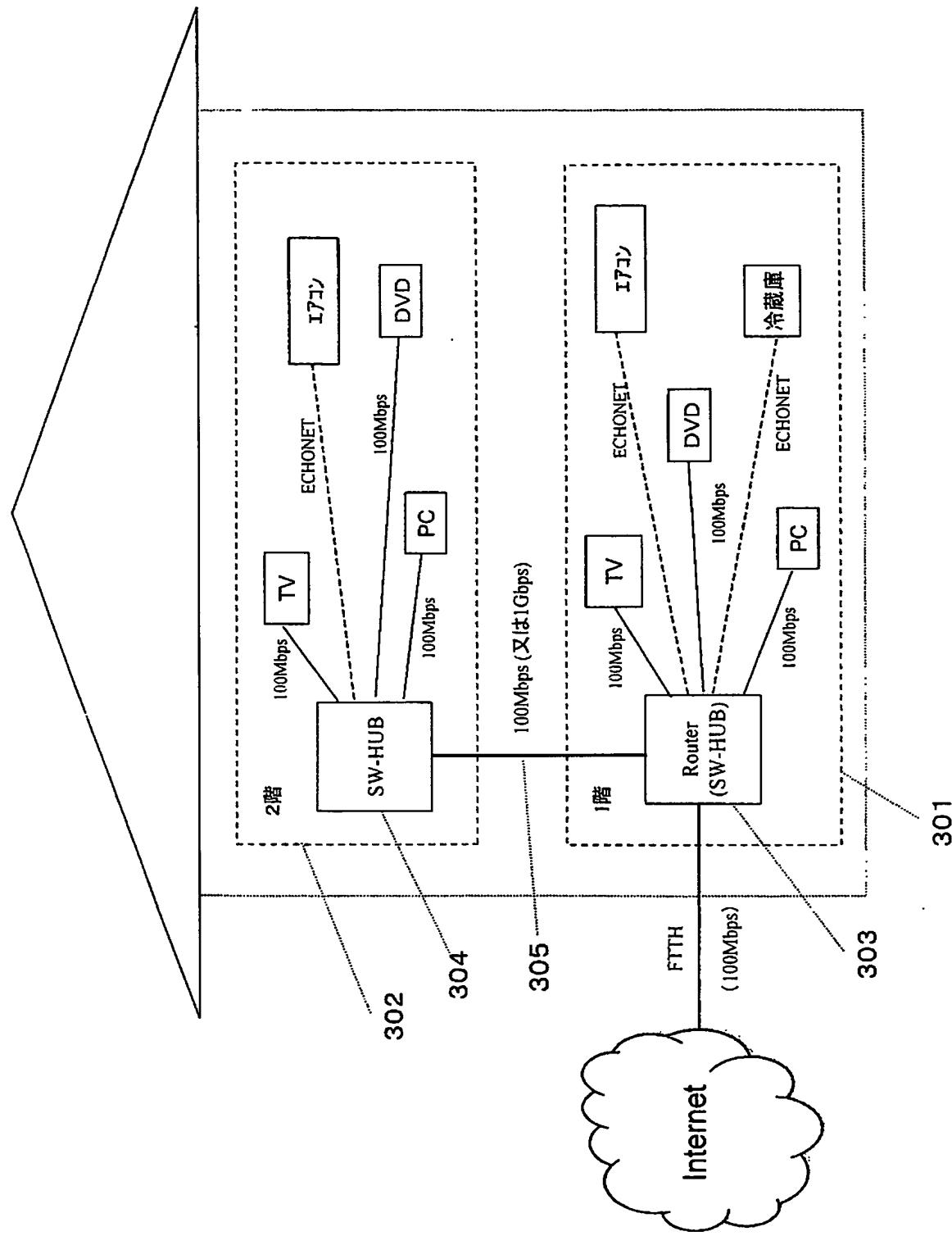
【図 1】



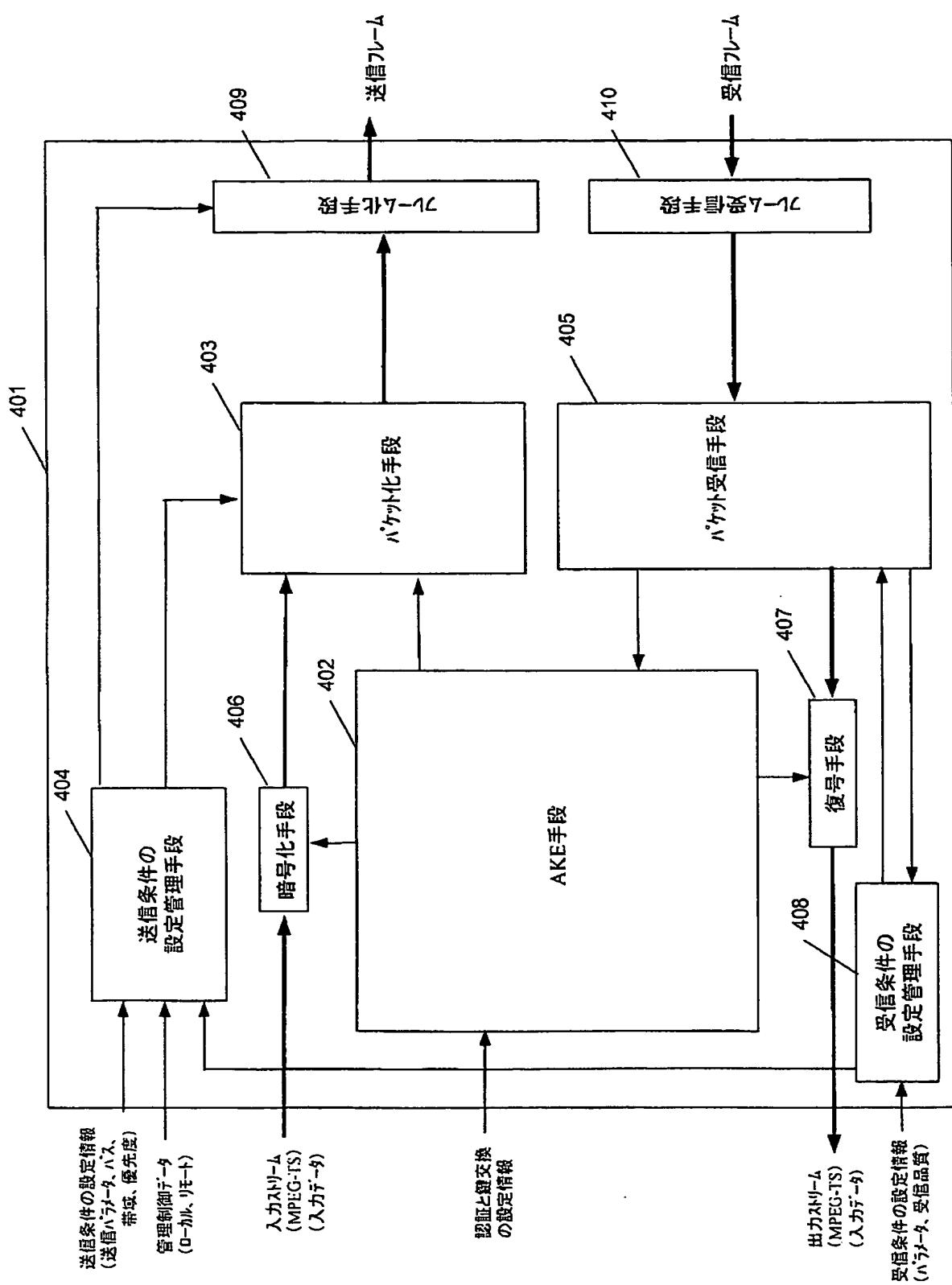
【図2】



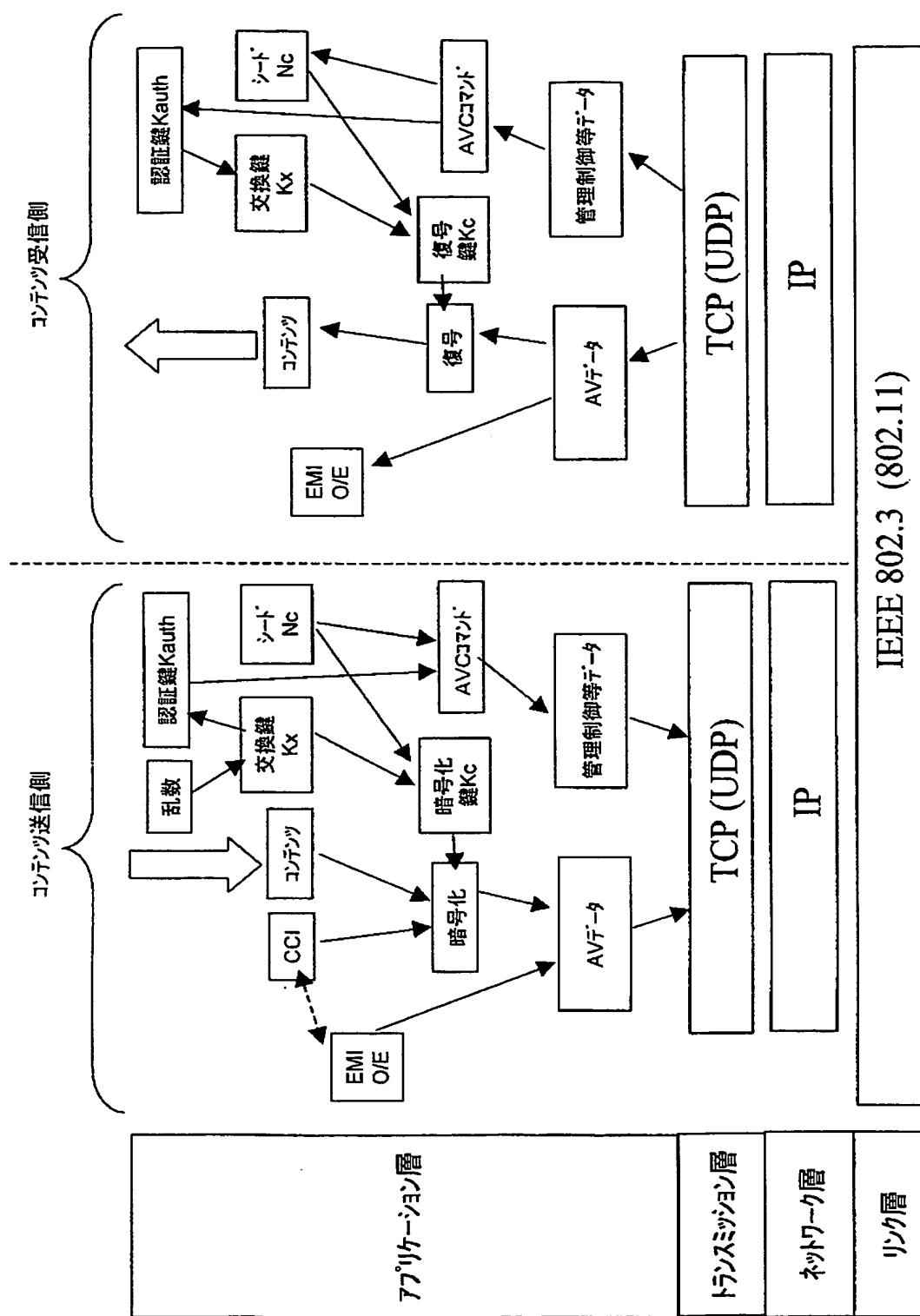
【図3】



【図4】

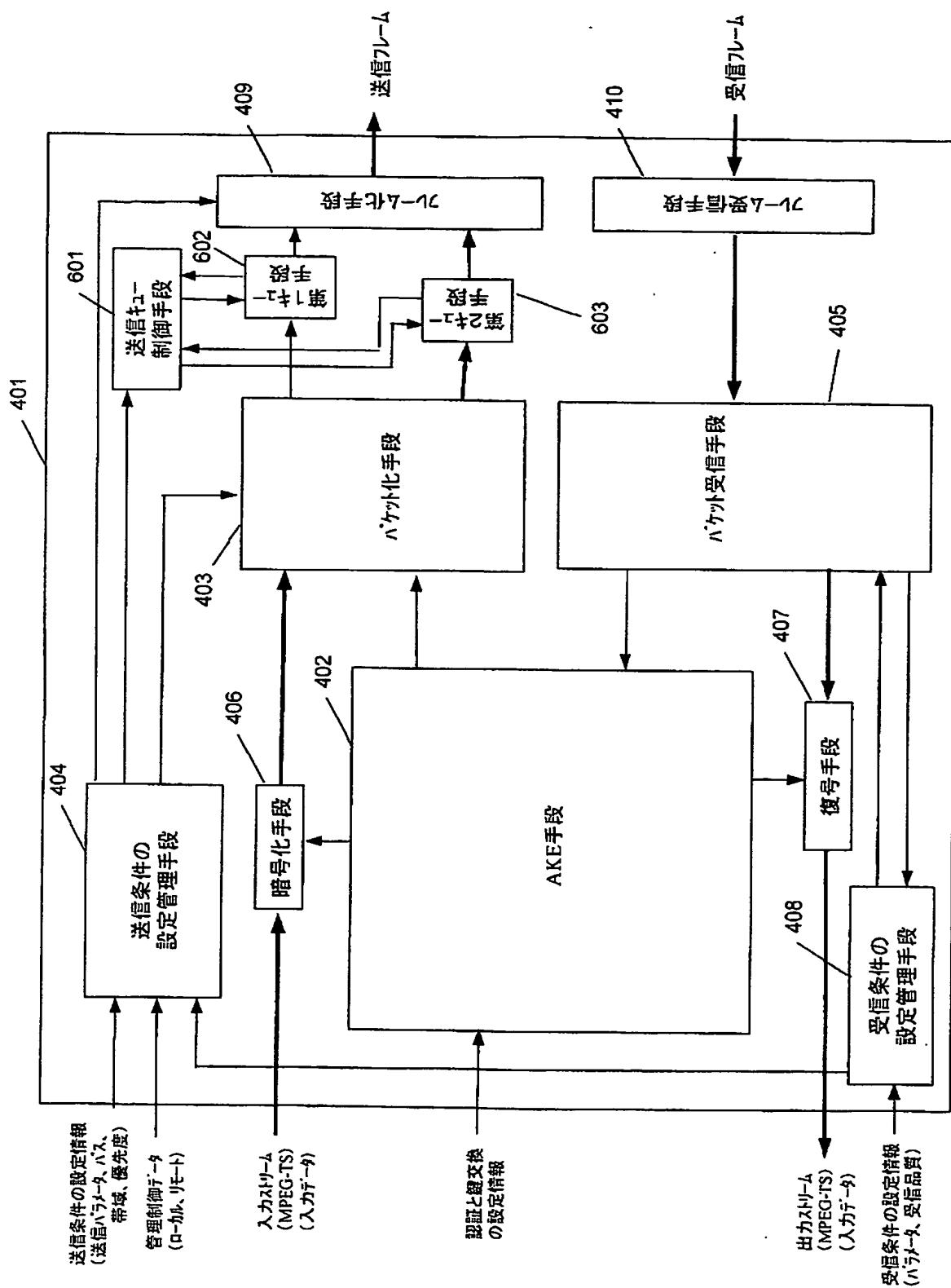


【図 5】

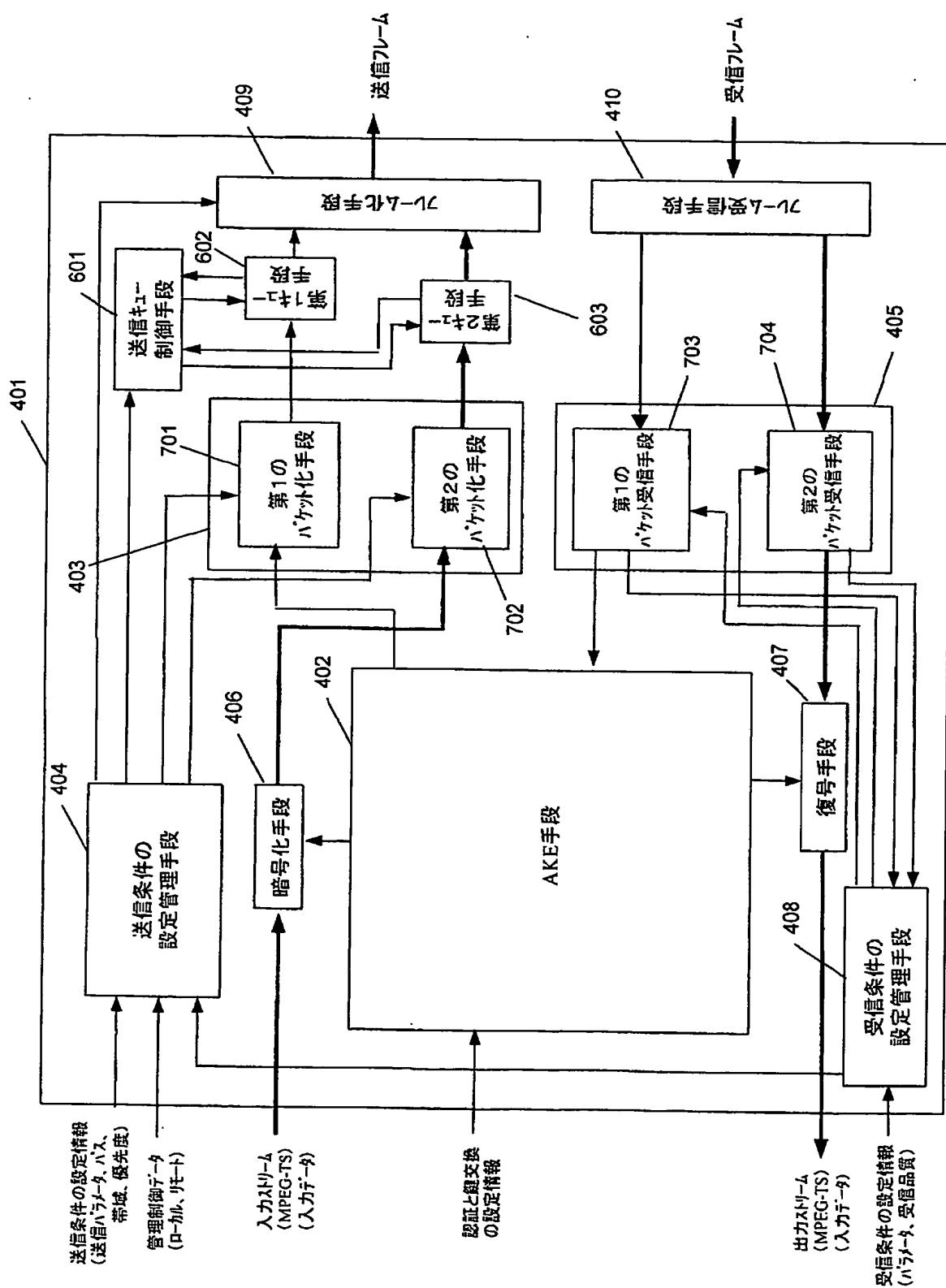


(OSIモデルによる説明)

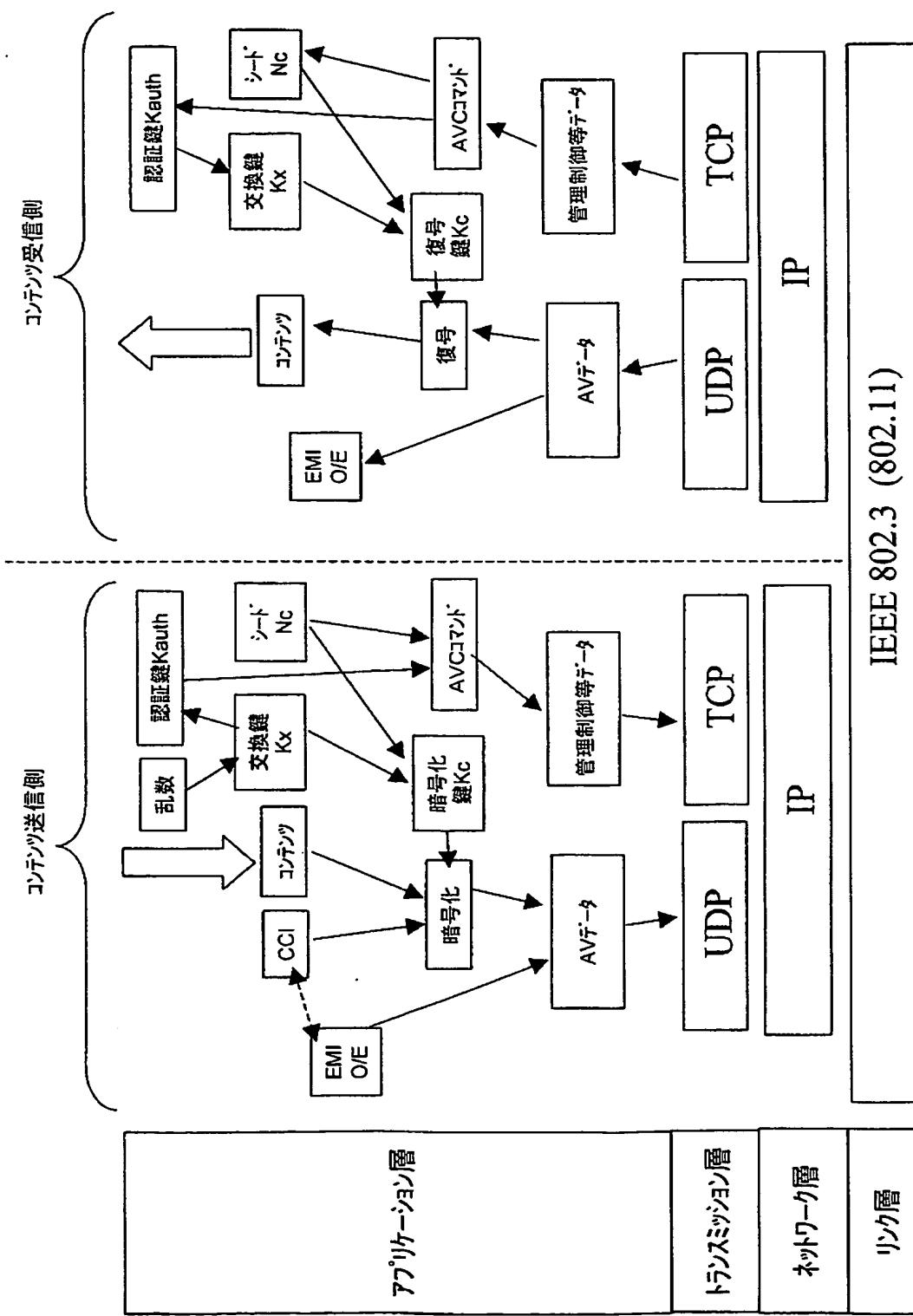
【図 6】



【図 7】

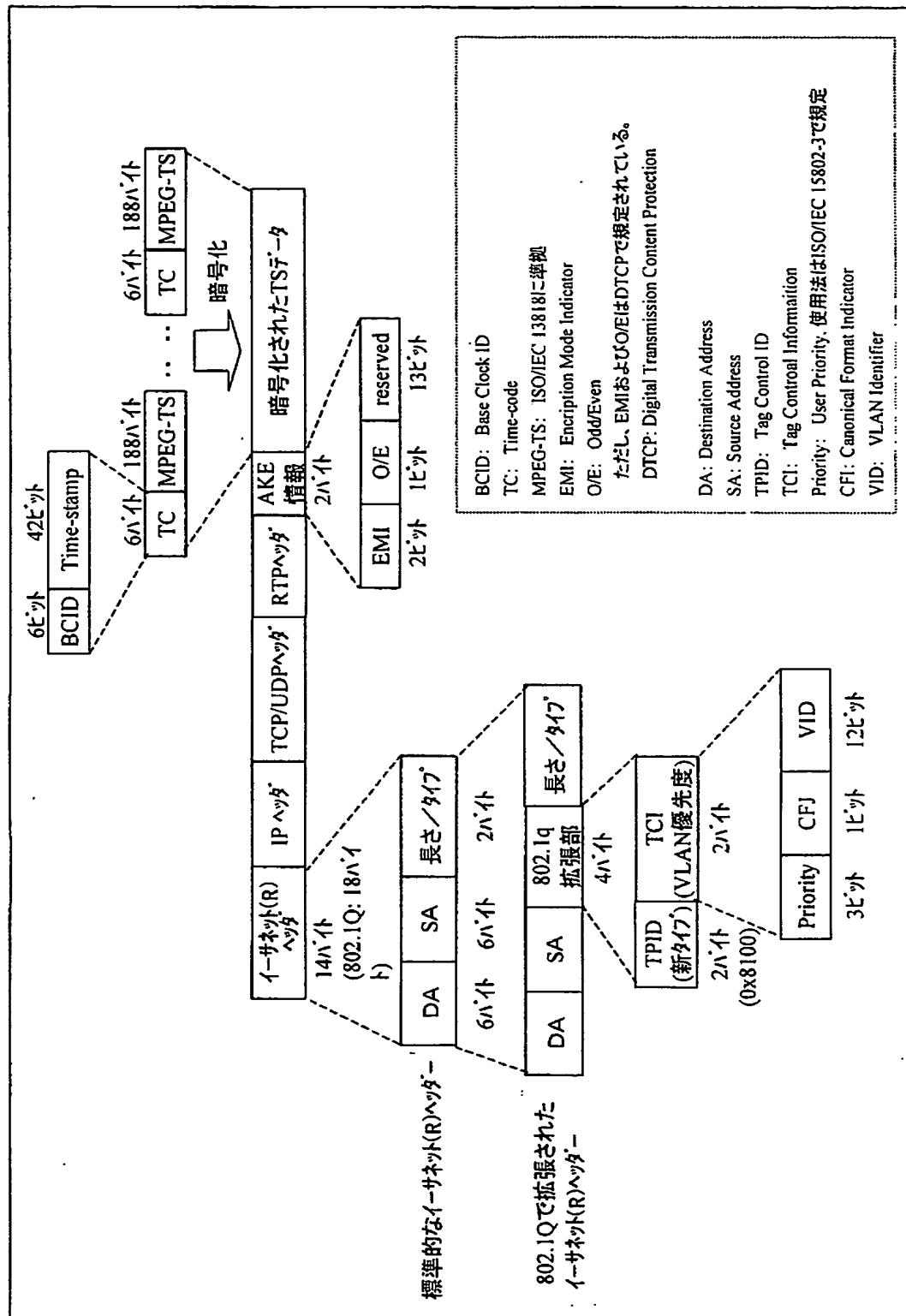


【図 8】

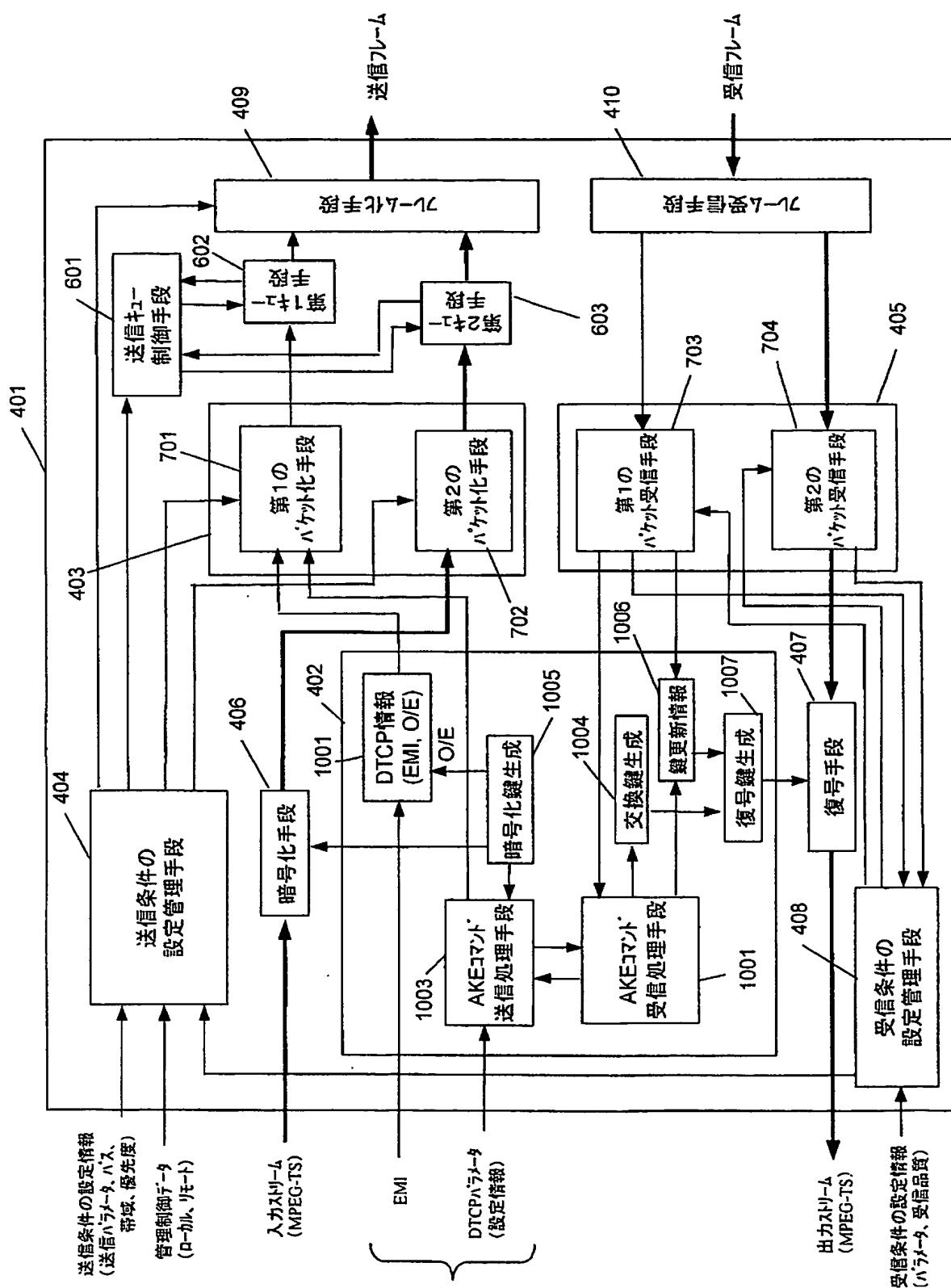


(OSIモデルによる説明)

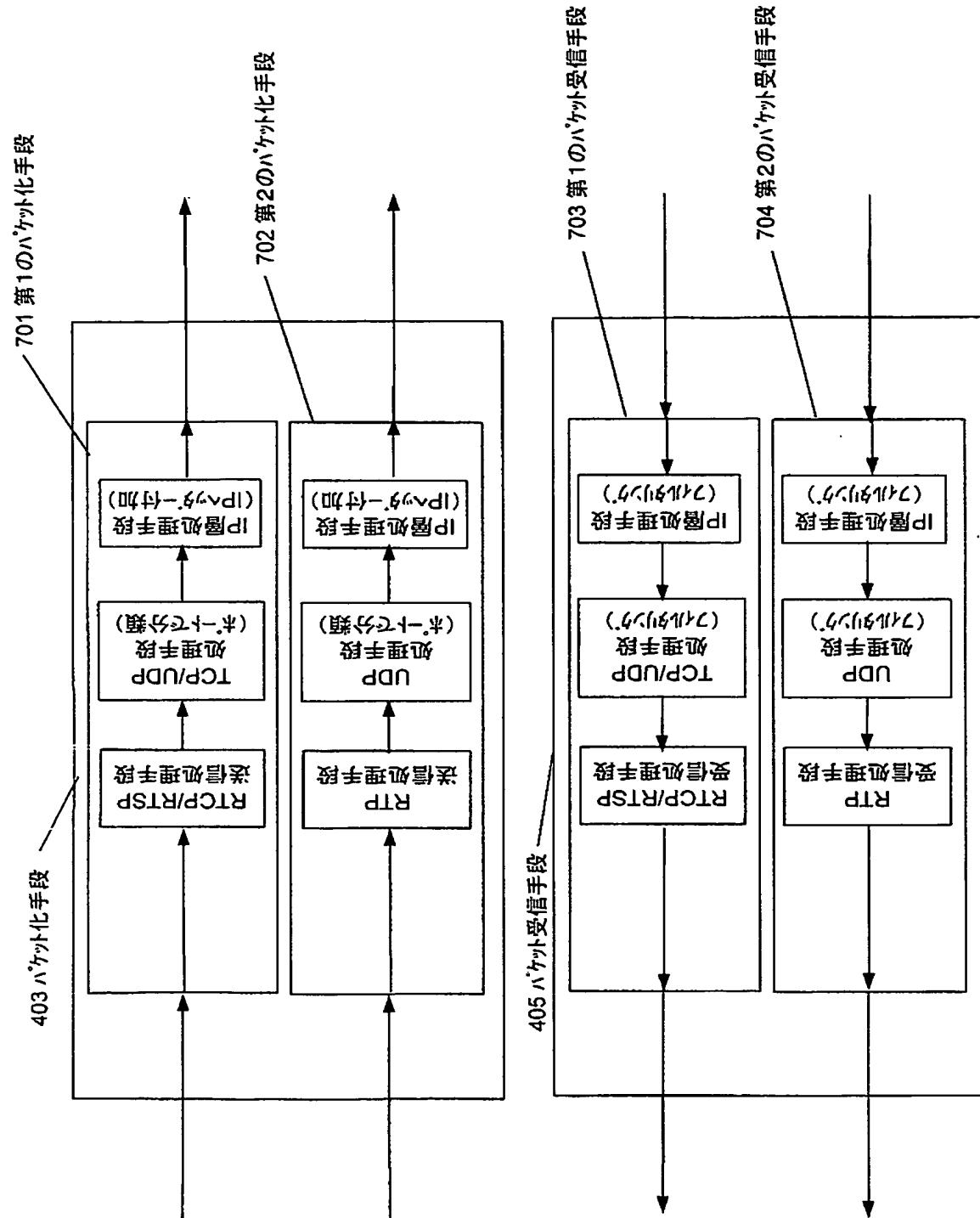
【図9】



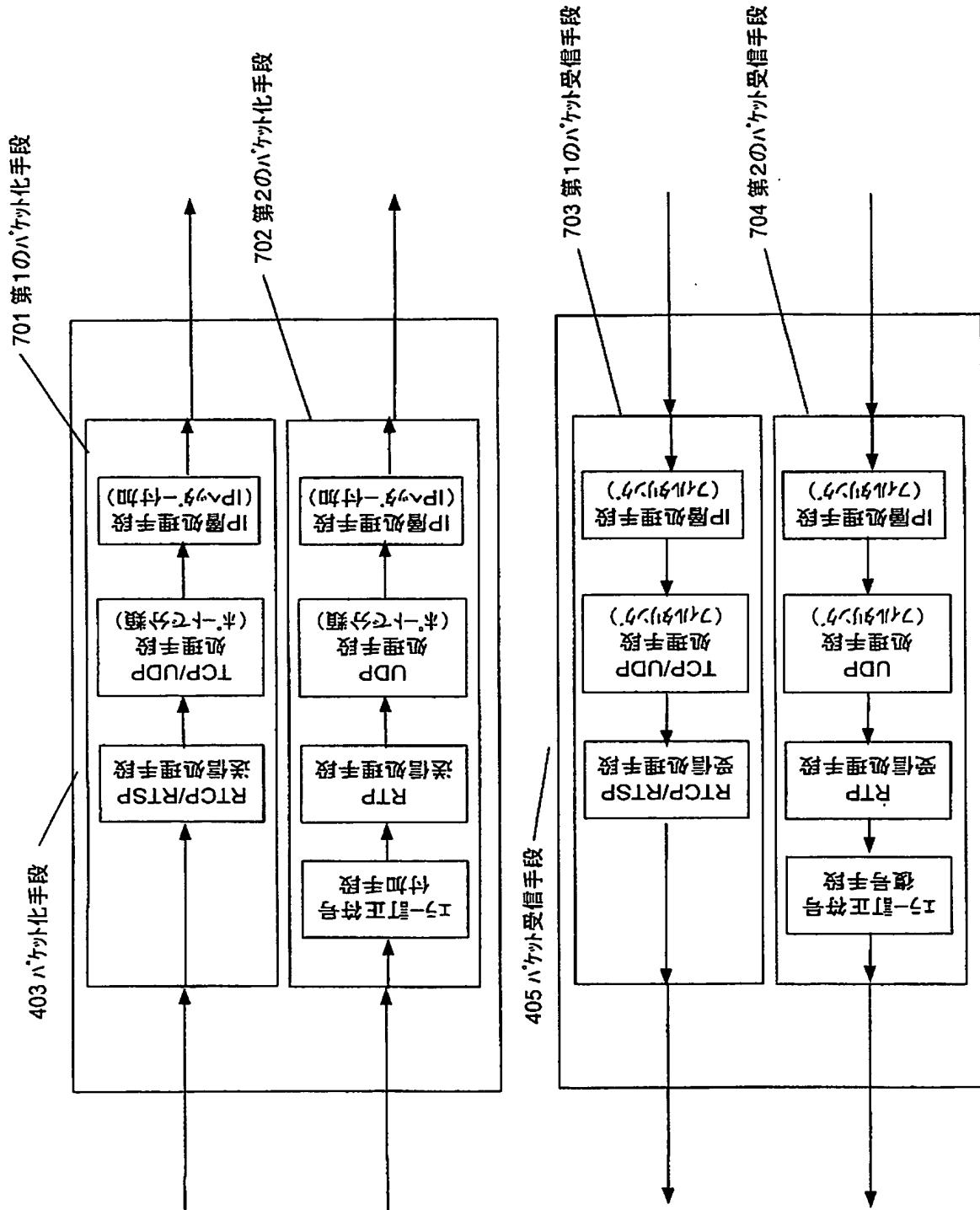
【図 10】



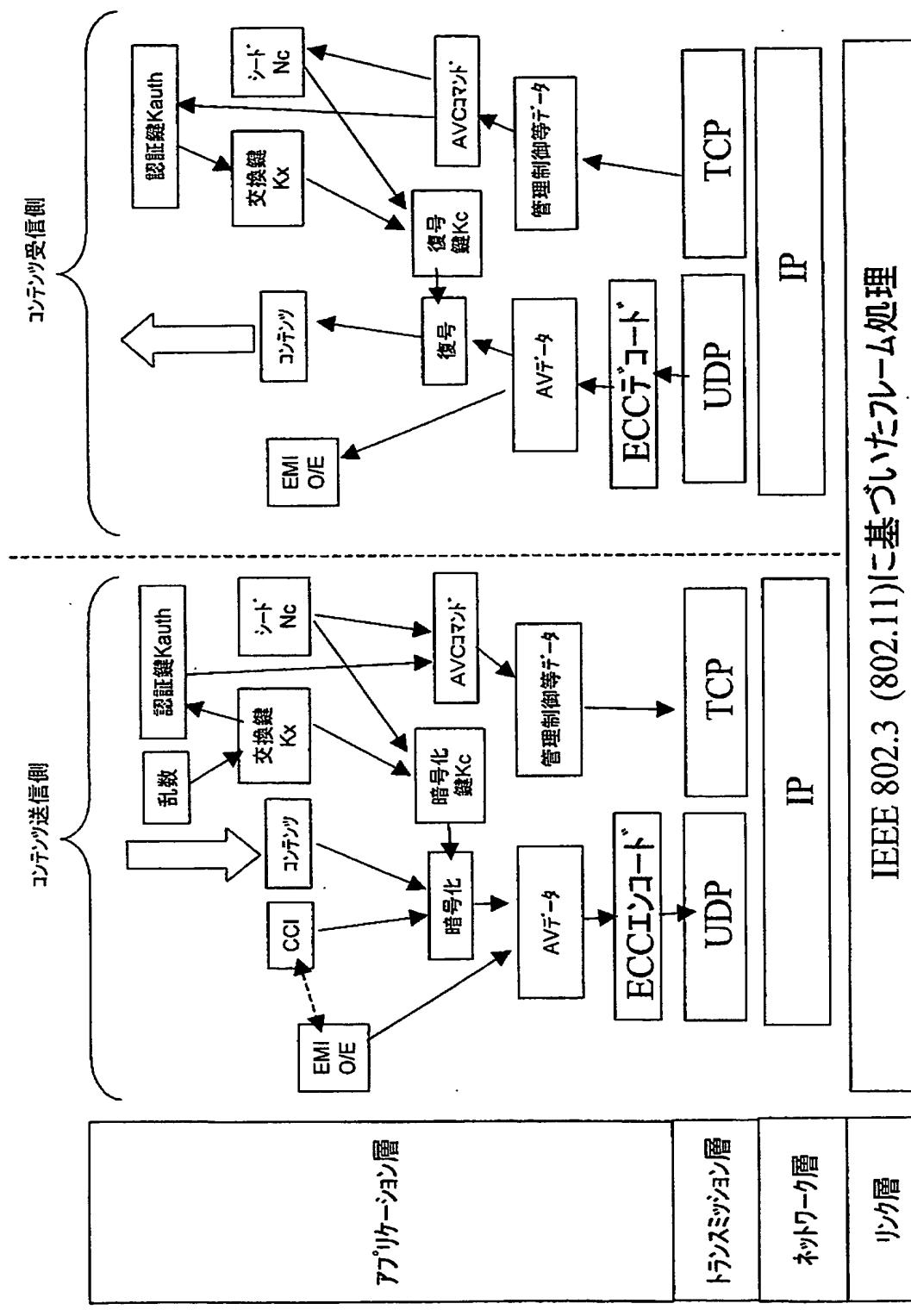
【図 11】



【図12】

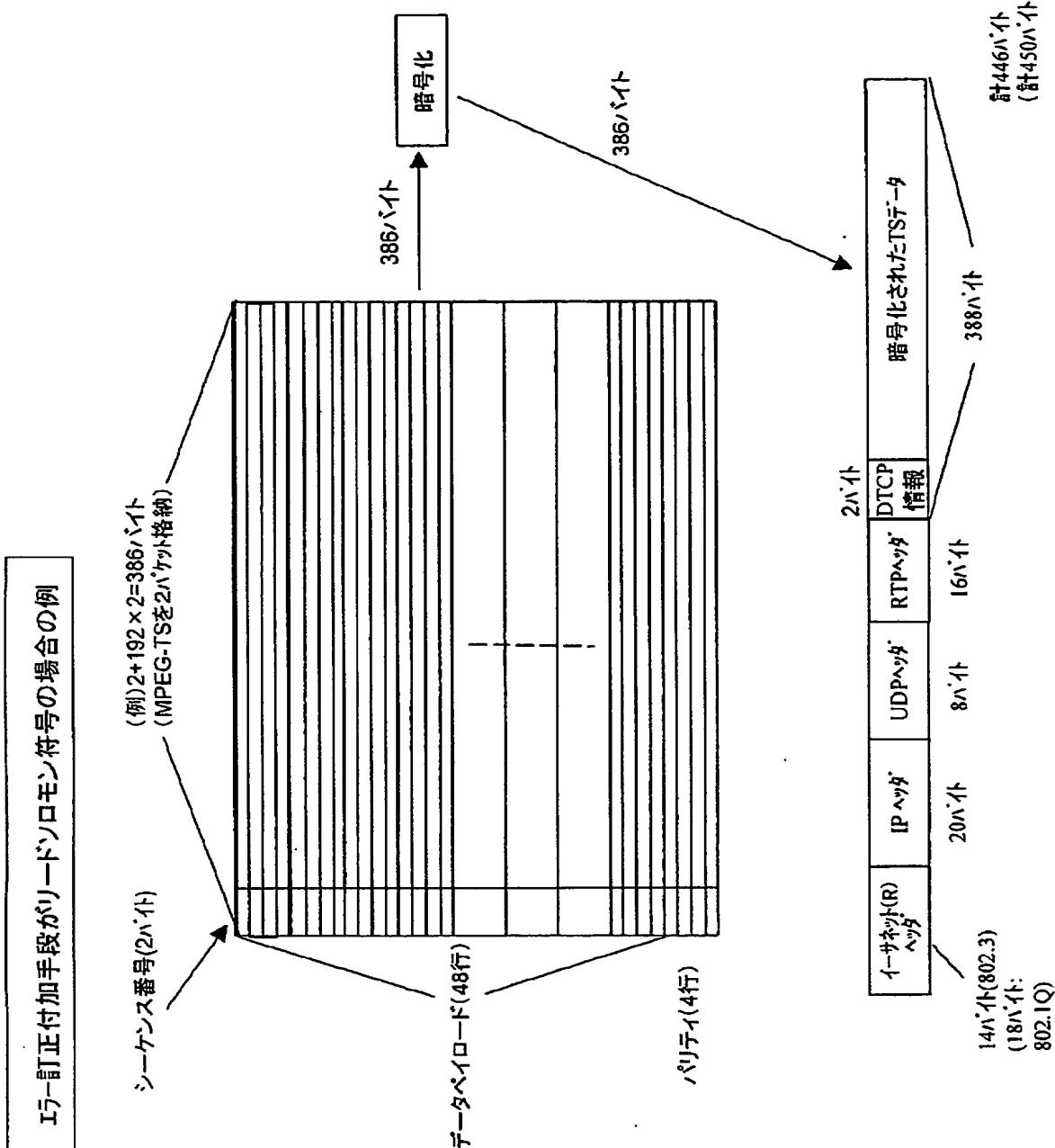


【図 13】

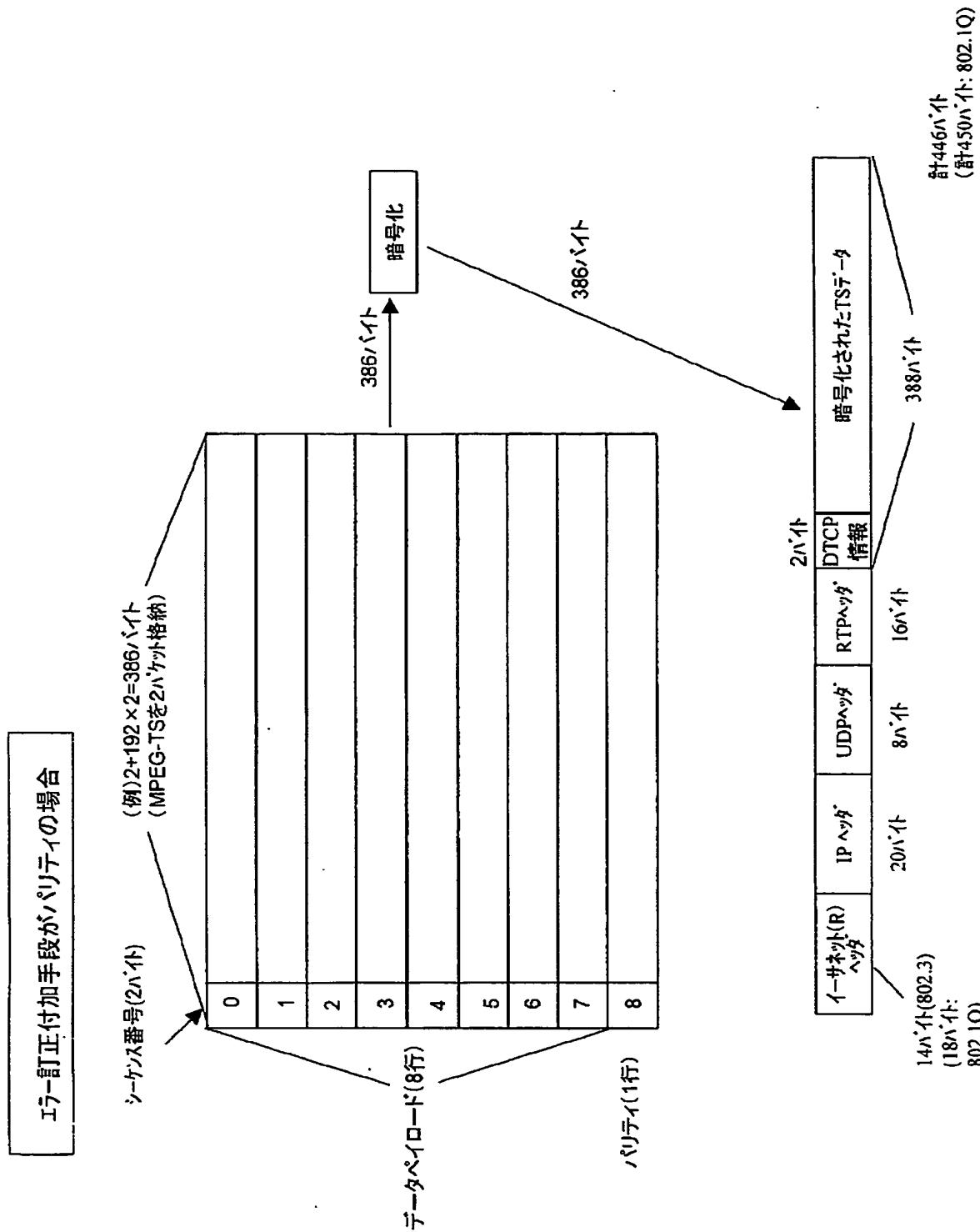


(OSI モデルによる説明)

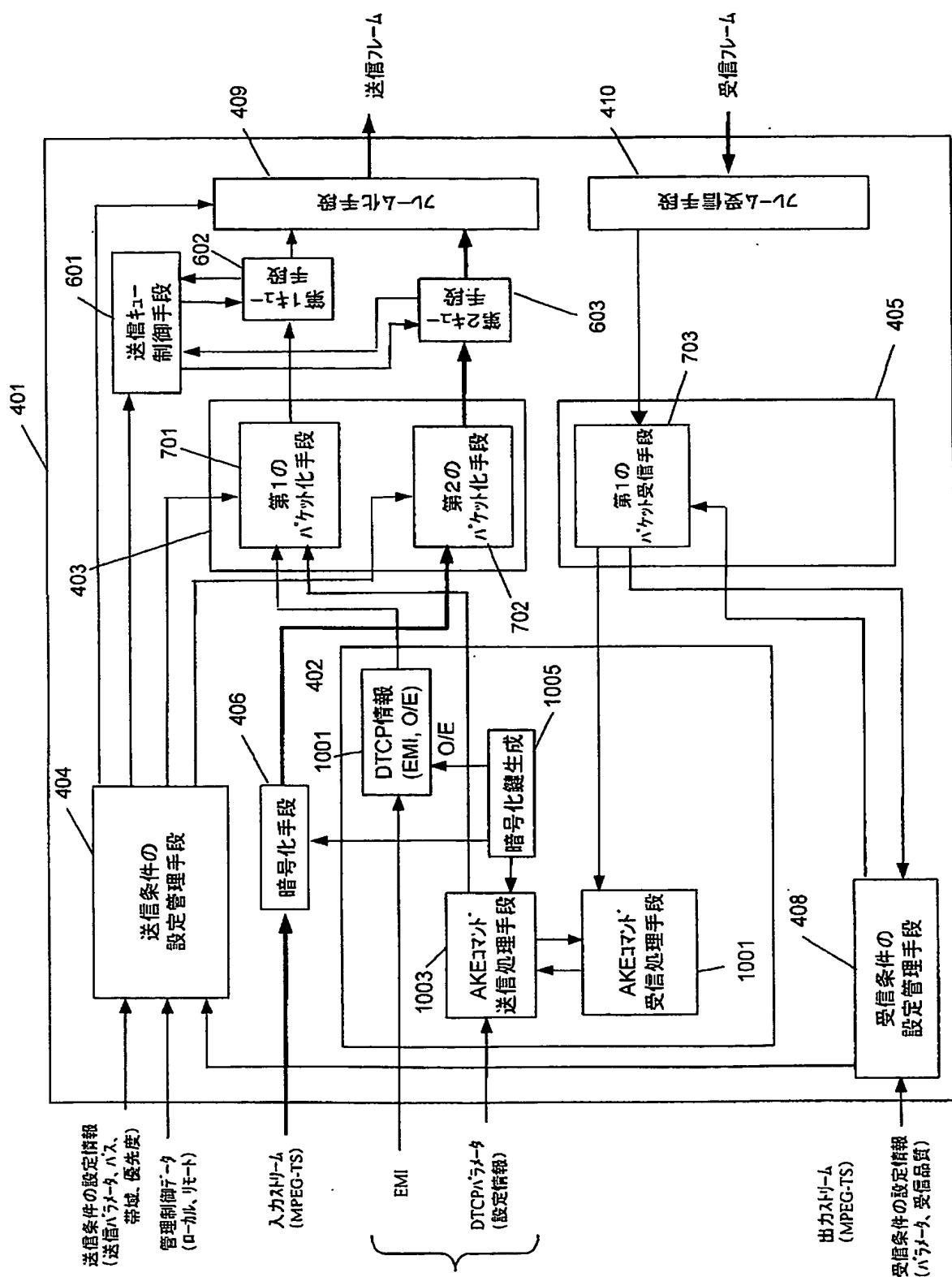
【図14】



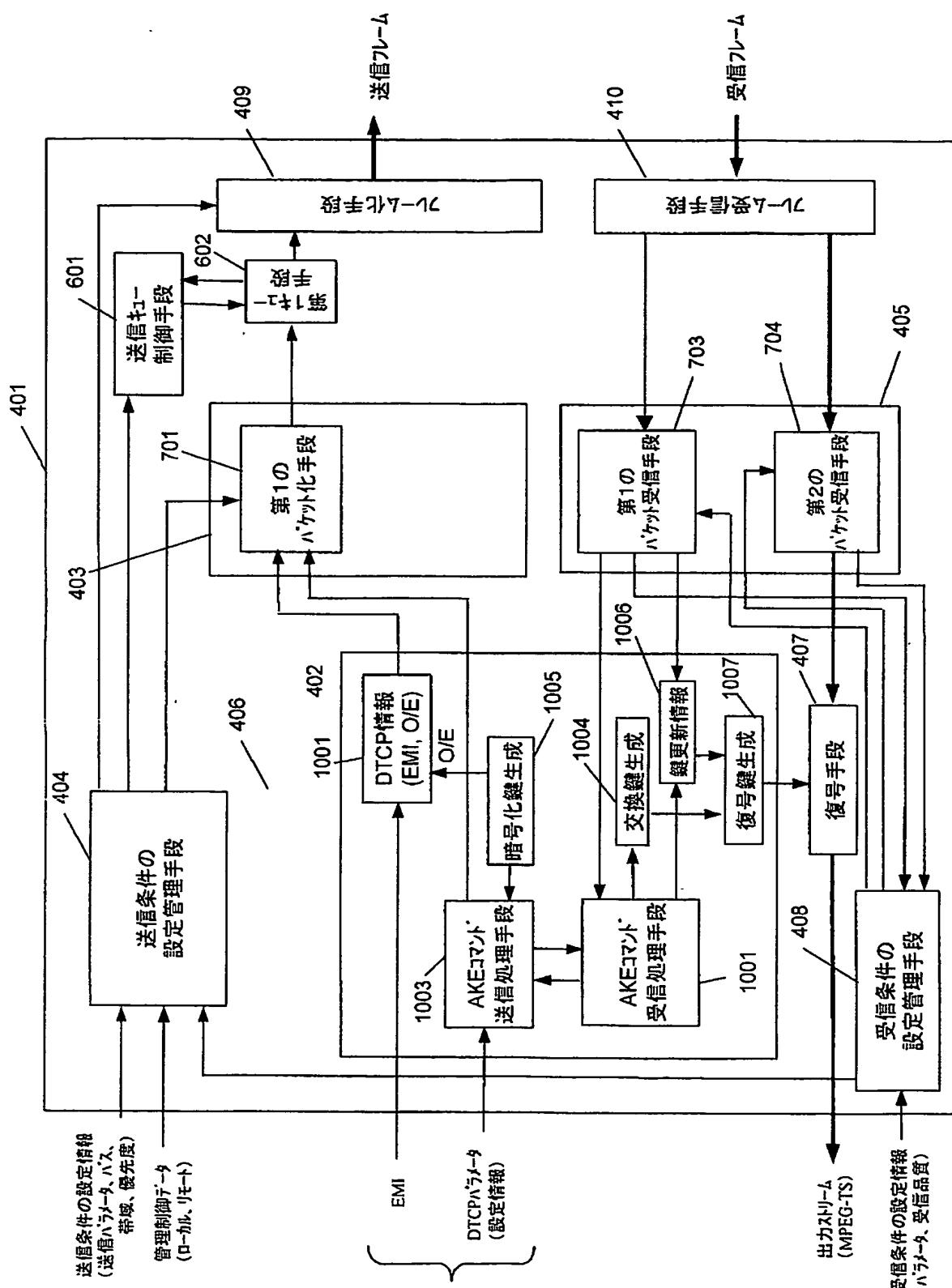
【図 15】



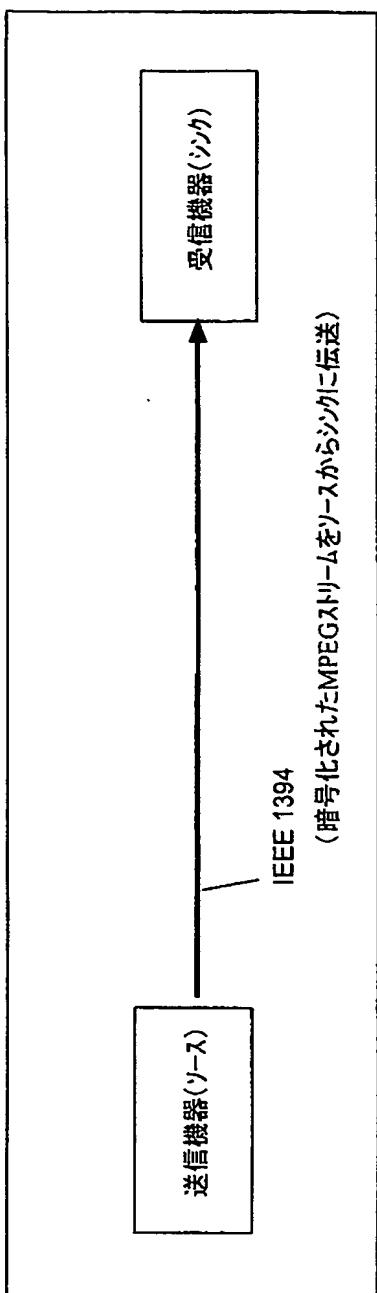
【図16】



【図 17】



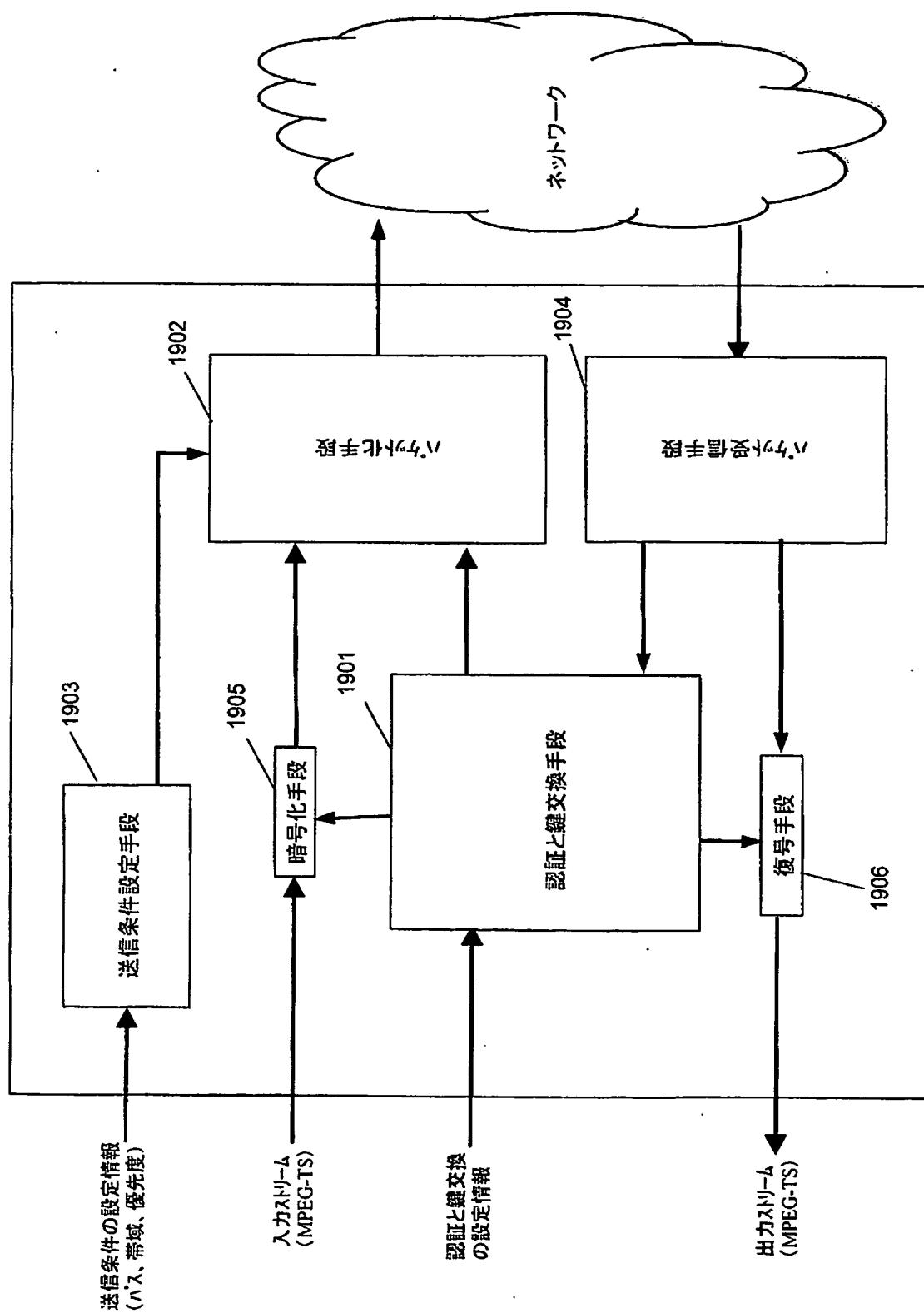
【図18】



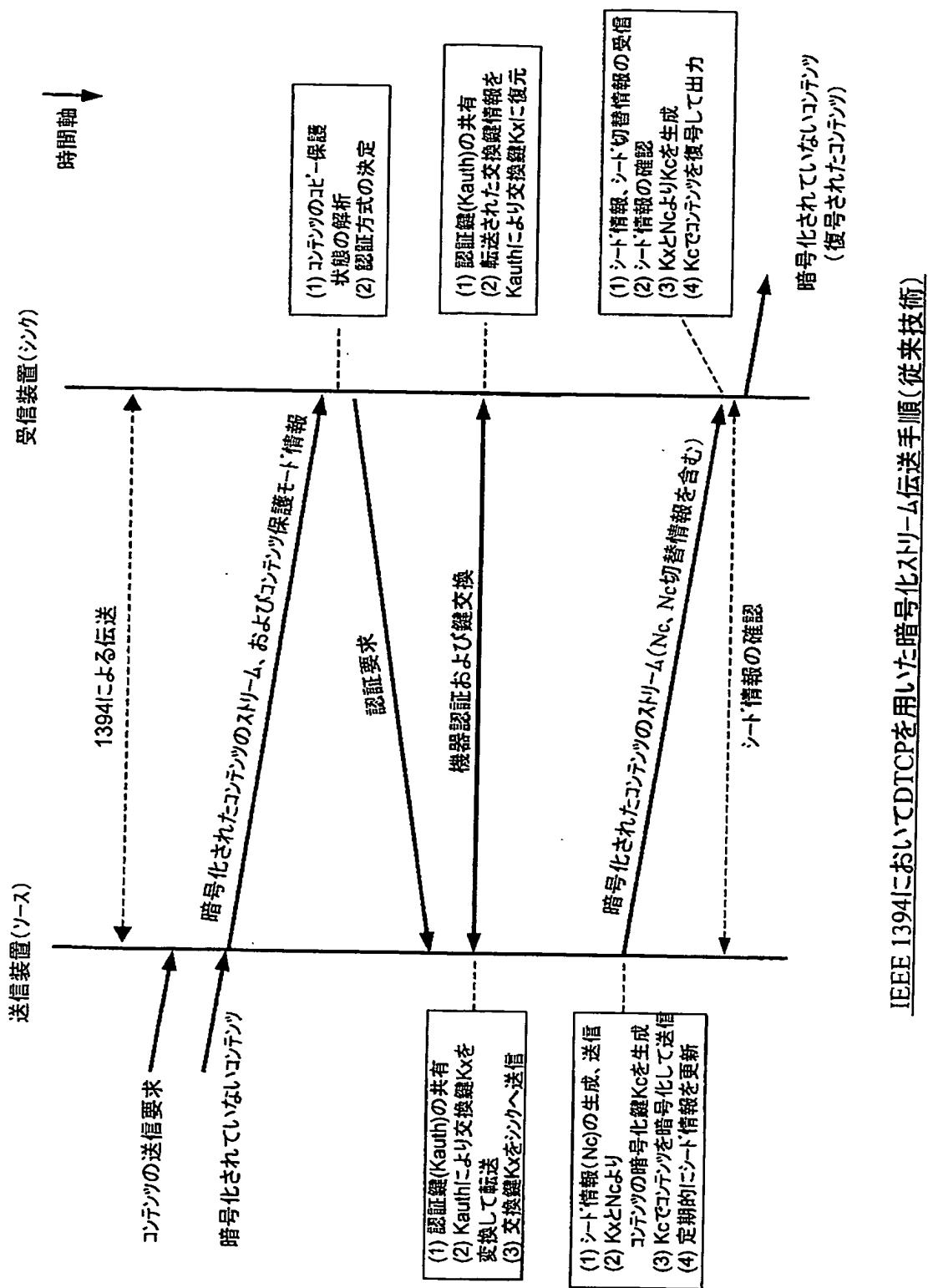
送信機器(ソース)の例	受信機器(シルク)の例	コンテンツ伝送における暗号化
DVHS	DVHS	
HDDレコーダ	HDDレコーダ	MPEG-TSにDTCP方式によるコンテンツ保護を実施
1394搭載STB	1394搭載STB	
1394搭載デジタルTV	1394搭載デジタルTV	

IEEE 1394においてDTCPを用いたMPEGストリームの伝送

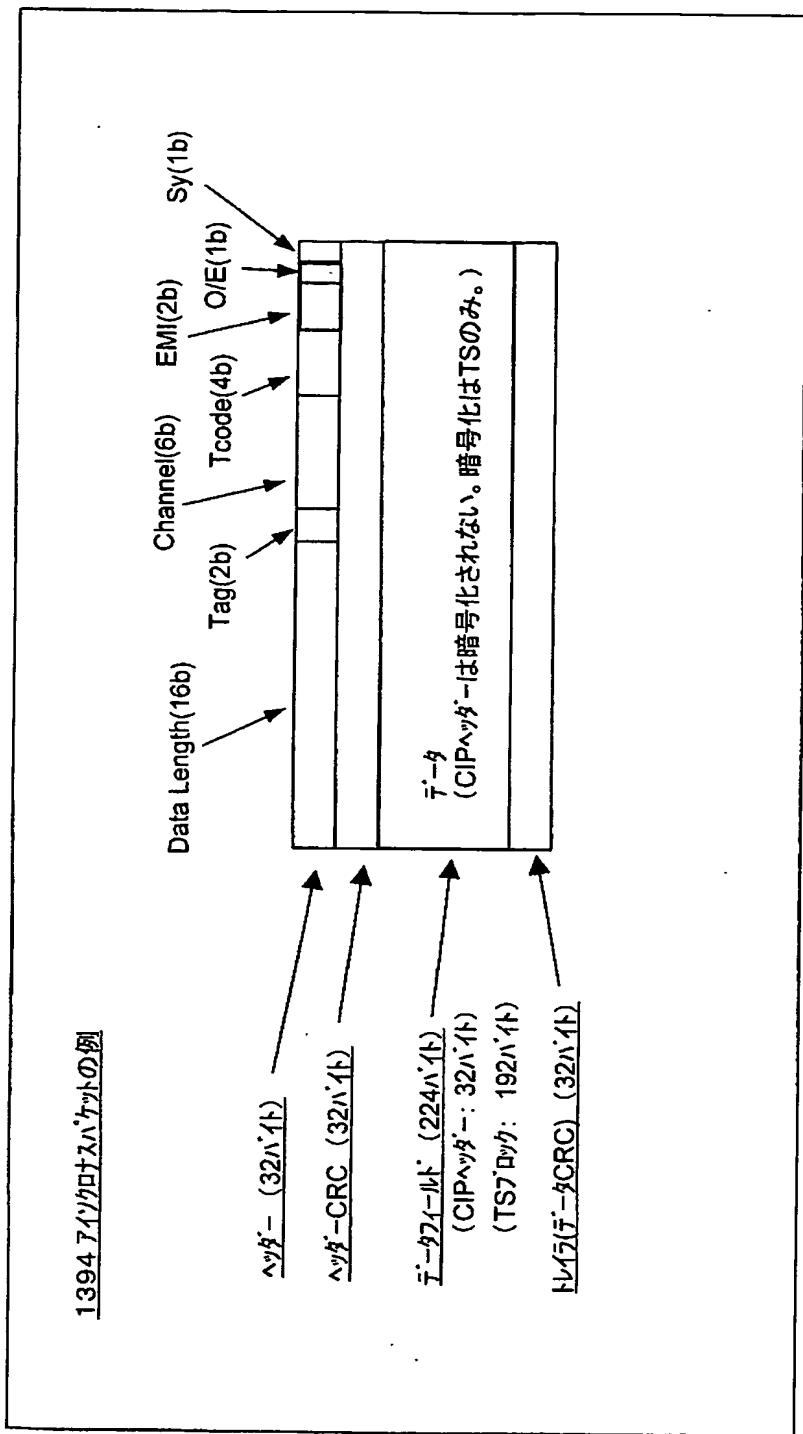
【図19】



【図 20】



【図 21】



【書類名】 要約書

【要約】

【課題】 M P E G - T S などの A V データを I P ネットワークを用いて伝送する場合に、伝送エラーや盗聴に強い高品質 A V コンテンツのリアルタイム伝送手段を実現する。

【解決手段】 ネットワークを介して論理的に接続された送信装置と受信装置は、送信データのセキュリティを確保するための機器認証と暗号化鍵の交換手段と、コンテンツの暗号化手段、および、暗号化されたコンテンツの復号手段と、受信側からフィードバックされるパケット受信状況を入力して適切なパケット送信条件を設定するパケット送信条件設定管理手段と、パケット化手段と、パケット受信手段と、パケット受信条件の設定管理手段とを具備する。これにより、M P E G - T S 信号などの A V ストリームを送信機器で暗号化して、データの機密性や著作権の保護を図りながら I P ネットワーク上を伝送し、受信機器で元の信号を復号することが可能である。

【選択図】 図 4

特願 2002-340582

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- INES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.